NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

AN ANALYSIS OF THE FEASIBILITY AND APPLICABILITY OF IEEE 802.X WIRELESS MESH NETWORKS WITHIN THE GLOBAL INFORMATION GRID

by

Eric J. Bach
Mark G. Fickel

September 2004

Thesis Advisor: Alexander Bordetsky
Second Reader: Brian Steckler

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: An Analysis of the Feasibility and Applicability of IEEE 802.x Wireless Mesh Networks within the Global Information Grid			**5. FUNDING NUMBERS**
6. AUTHOR(S) Eric J. Bach, Mark G. Fickel			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

This thesis analyzes the feasibility, functionality, efficacy and usability of IEEE 802.x wireless mesh networks in multiple DoD contexts. Through multiple field and lab experiments and hardware investigations, an assessment is performed on the realistic implementation issues of wireless mesh networks and their possible applications. A detailed examination is conducted of the variable elements, operational constraints, and possible decision points for developing a usable, robust, self-organizing, wireless mesh network that can be leveraged for maximum usability and shared situational awareness in network-centric operations. The research investigates the suitability of currently available COTS hardware and software wireless mesh networking components for geographically distributed networks. Additionally, a product-line software architecture and a common data interchange XML vocabulary are proposed as the enabling technology elements to carry application layer mesh forward for integration of collaborative sensor-decision maker adaptive networks within the Global Information Grid. The thesis includes the design and implementation of the first Naval Postgraduate School testbed for tactical level mesh networking with unmanned vehicles, unattended sensors, and warrior networking nodes. This thesis also lays the groundwork for further research into lower OSI-layer routing protocols for DoD mesh networks, development of mesh-aware applications, as well as a GIG-wide mesh network architecture.

14. SUBJECT TERMS Wireless Mesh Networking, Ad Hoc Networking, IEEE 802.11, IEEE 802.16, IEEE 802.15.4, Global Information Grid, Mesh Networking Markup Language, MeshNetML, Wireless, MANET, Sensor Networks, Mesh Routing and Capabilities Toolset, MERCAT			**15. NUMBER OF PAGES** 115
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

AN ANALYSIS OF THE FEASIBILITY AND APPLICABILITY OF IEEE 802.X WIRELESS MESH NETWORKS WITHIN THE GLOBAL INFORMATION GRID

Eric J. Bach
Lieutenant Commander, Supply Corps, United States Navy
B.S., United States Naval Academy, 1993

Mark G. Fickel
Lieutenant Commander, United States Navy
B.S., South Dakota School of Mines and Technology, 1987

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2004

Author: Eric J. Bach

Mark G. Fickel

Approved by: Alexander Bordetsky
Thesis Advisor

Brian Steckler
Second Reader

Dan Boger, Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis analyzes the feasibility, functionality, efficacy and usability of IEEE 802.x wireless mesh networks in multiple DoD contexts. Through multiple field and lab experiments and hardware investigations, an assessment is performed on the realistic implementation issues of wireless mesh networks and their possible applications. A detailed examination is conducted of the variable elements, operational constraints, and possible decision points for developing a usable, robust, self-organizing, wireless mesh network that can be leveraged for maximum usability and shared situational awareness in network-centric operations. The research investigates the suitability of currently available COTS hardware and software wireless mesh networking components for geographically distributed networks. Additionally, a product-line software architecture and a common data interchange XML vocabulary are proposed as the enabling technology elements to carry application layer mesh forward for integration of collaborative sensor-decision maker adaptive networks within the Global Information Grid. The thesis includes the design and implementation of the first Naval Postgraduate School testbed for tactical level mesh networking with unmanned vehicles, unattended sensors, and warrior networking nodes. This thesis also lays the groundwork for further research into lower OSI-layer routing protocols for DoD mesh networks, development of mesh-aware applications, as well as a GIG-wide mesh network architecture.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACRONYMS AND ABBREVIATIONS

ACK	Acknowledge
AODV	Ad Hoc On-demand Distance Vector
AP	Access Point
BRP	Bordercast Routing Protocol
COTS	Commercial Off-The-Shelf
DAN	Device-Aware Networking
DARPA	Defense Research Projects Agency
DoD	Department of Defense
DSR	Dynamic Source Routing
ESS	Extended Service Set
FSR	Fisheye State Routing
GIG	Global Information Grid
GIGA	Global Information Grid Applications
GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
IARP	Intrazone Routing Protocol
IBSS	Independent Basic Service Set
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IERP	Interzone Routing Protocol
IETF	Internet Engineering Task Force
IIS	Internet Information Server

IPv6	Internet Protocol Version 6
LANMAR	Landmark Ad Hoc Routing
LSP	Link State Packet
MAC	Media Access Control
MANET	Mobile Ad Hoc Network
MAR	Mobile Access Router
MCN	Model-based Communication Network
MERCAT	Mesh Routing and Capabilities Toolset
MeshNetML	Mesh Network Markup Language
MID	Multiple Interface Declaration
MMBDP	Mobile Mesh Border Discovery Protocol
MMLDP	Mobile Mesh Link Discovery Protocol
MMRP	Mobile Mesh Routing Protocol
MobileIP	Mobile Internet Protocol
MPR	Multipoint Relay
NAP	Network Access Points
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
NPS	Naval Postgraduate School
NRL	Naval Research Laboratory
OFDM	Orthogonal Frequency Division Multiplexing
OID	Object Identifier
OLSR	Optimized Link State Routing

OSI	Open System Interconnection
PAR	Project Authorization Request
PCMCIA	Personal Computer Memory Card International Association
PHY	Physical
PWRP	Predictive Wireless Routing Protocol
QoS	Quality-of-Service
RAM	Random Access Memory
RERR	Route Error
RF	Radio frequency
RFC	requests for comments
RREP	Route Reply
RREQ	Route Request
SA	Situational Awareness
SensorML	Sensor Modeling Language
SNMP	Simple Network Management Protocol
STAN	Surveillance and Target Acquisition Network
SYN	Synchronize
TBRPF	Topology dissemination Based on Reverse-Path Forwarding
TCO	Total Cost of Ownership
TND	TBRPF Neighbor Discovery
TOC	Tactical Operations Center
UGS	Unattended Ground Sensors
UML	Uniform Modeling Language
VIRT	Valued Information at the Right Time

VoIP	Voice over Internet Protocol
WAP	Wireless Access Point
WDS	Wireless Distribution System
WiFi	Wireless Fidelity
WISP	Wireless Internet Service Providers
WPAN	Wireless Personal Area Network
XML	Extensible Markup Language
ZRP	Zone Routing Protocol

ACKNOWLEDGMENTS

We would like to acknowledge and thank Dr. Alex Bordetsky for all the support, patience, and encouragement you provided throughout our journey. You allowed us the freedom to work toward our research vision every step of the way. We would also like to acknowledge the contributions and assistance of the GIGA Lab team, specifically Axel Schumann and Ryan Blazevich. Your professionalism, drive, and thirst for knowledge helped make the mesh a reality. Fair winds and following seas!

Lieutenant Commander Eric J. Bach:

To my beautiful wife Kazumi, thank you for making the enormous sacrifices you made for me each and every day. Your love is a gift that I cherish and which gave me the strength to see my mesh dream through.

To my son Eric Jiei, thank you simply for being born and showing me that every minute of life is a blessing. Finally, thank you to my daughter-to-be, Minami Erika, for bringing even more joy and inspiration into my world.

Lieutenant Commander Mark G. Fickel:

First, I would like to thank God for the many blessings in my life. Words could never express how grateful I am for the opportunities afforded me by my Lord and Savior, Jesus Christ.

To my parents, Monty and Gerry Fickel, thank you for standing by me through all my endeavors. Your wisdom is unequaled, your support inexhaustible, and your love unwavering.

To Kevin and Carolyn O'Donnell, thank you for your boundless encouragement and sage advice.

To my thesis partner, Eric Bach, thank you for your untiring dedication to our many projects here at NPS, including our thesis. Your drive for excellence is truly inspirational. Some of the most fulfilling moments of my graduate experience were our late-night discussions, study sessions, and dreaming up and completing experiments with you.

And last, but certainly not least, a deeply heartfelt thanks to my wonderful family, the center of my universe, and the reason I strive for perfection. To my beautiful children, Matthew, Elizabeth, and my yet-unborn son, thank you for keeping me on my toes and never letting me forget about the most important things in life. To my lovely wife, Colleen, thank you for your unquestioning love, ceaseless encouragement, infinite patience, and immeasurable support in all things. My achievements would mean nothing without you beside me. You remain my best friend, my partner, and my love.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Wireless networking has emerged as a popular network architecture solution for many diverse situations and environments. Traditional point-to-point or point-to-multipoint wireless networks are constrained, however, by the requirement to have access points connected to the wired network for backhaul to a larger network or the global Internet. This access point paradigm limits the travel distance of individual nodes to the radio range of the wireless radios in use. A multipoint-to-multipoint architecture, in which every node becomes a router within the network, is a way to enable larger coverage distances with less investment.

True wireless ad hoc mesh networks are self-organizing, self-healing, self-balancing and, most importantly, self-aware. The central idea that enables mesh networking is the idea of dynamic, node-based routing. Self-organizing networks form when every node has the capability to join and create a network automatically upon discovering nodes with a similar capability within its radio range. Each node will have network awareness of its surrounding landscape and will be able to make efficient information path decisions as a result. If routes to other nodes are degraded or lost, better paths will be chosen "on the fly." The more end-user nodes that are added, the stronger the lattice of the mesh becomes as more routes become available to share the network load. Load-balancing and route control functions are shifted from dedicated network routers back onto the routing clients of the mesh. Effective construction of the lower OSI-layer mesh will depend on choosing the best routing algorithm for physical structure and behavior of the nodes.

Once the underlying substrate of the wireless mesh is established, application layer possibilities begin to emerge that may have great implications for the Global Information Grid (GIG) and the Department of Defense (DoD) systems of the future.

B. OBJECTIVES

This thesis is intended to lay the groundwork for future study of mobile ad hoc and wireless mesh networking topics related to the Department of Defense's Global

Information Grid environment. The GIG is the, "globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel."[1]

The objective of this research is to outline current challenges of creating a ubiquitous, standards-based mesh network across the GIG; as well as too investigate possible steps to take to move toward that lofty goal.

An evaluation of the current mesh networking, commercial-off-the-shelf, standards-based hardware and software in order to create an initial topology of available technology is integral to future work in this area.

The benefits of this research are threefold. First, by conducting a detailed examination of new technology that may be usable in critical operating environments in which traditional wired and wireless network deployment is infeasible or not cost effective, we have attempted to begin the work of picking a "best of breed" collection of components to build the mesh segments of the Global Information Grid. Second, by creating a testbed for follow-on research, we have established physical and logical tools to allow for a more in-depth study of wireless mesh technologies by future Naval Postgraduate School (NPS) students. Finally, by creating a new paradigm of application layer mesh as an enabler for users of the GIG, we have charted a path for the future development of usable mesh components that are intended to be open and interoperable across the DoD information systems spectrum.

C. RESEARCH QUESTIONS

Our primary research question explores what the variable elements, operational constraints, and possible decision points are for developing a usable, robust, self-organizing, wireless mesh network that can be leveraged for maximum usability and shared situational awareness in network-centric operations. Additionally, we sought to determine what commercial off-the-shelf (COTS) technologies might be best suited for adaptation into a network-centric architecture. Based on that model, we examined the

[1] Department of Defense Directive 8100.1, "Global Information Grid Overarching Policy." Dated 19 September 2002, 8.

composition and behavioral characteristics of a usable, prototypical mesh testbed. Finally, we attempted to draw a conclusion about what application layer mesh networking will mean to users of the GIG.

D. SCOPE

The scope of this thesis is purposefully wide to create a foundation for further, follow-on research. It covers the analysis of implementation issues involved in the Institute of Electrical and Electronics Engineers (IEEE) 802.x standards-based wireless mesh networking solutions. Wireless security issues have been omitted simply because of the lack of maturity and fragility of the current mesh software implementations. A detailed study of Open System Interconnection (OSI) Layer 3 routing protocols is included as a first step toward better understanding the mechanisms that are used in multi-hop routing and as the jumping off point for an informal best-of-breed analysis. Layer 3, the network layer, of the Open System Interconnection (OSI) protocol model provides the technology and functionality for data transfer, routing, and internetworking between points on a network. Multiple field and laboratory experiments using currently available, commercial-off-the-shelf technologies form the basis of decision points that can be used for future architecture development decision making. An initial investigation of next-generation, application layer mesh approaches is also included in order to leverage the underlying network layer structure. A possible communications paradigm and data interchange mechanism that leverages the inherent behavioral characteristics of extended wireless mesh networks is proposed. Finally, wide-ranging recommendations are proffered based on our results and the momentum being gained by mesh networks around the world.

E. METHODOLOGY

Our methodology included extensive research of the available literature, both hard copy and electronic, on underlying mesh networking and Mobile Ad hoc Network (MANET) theory. We sought to conduct as wide an examination of the literature as possible to strengthen our knowledge on as many of the facets of wireless mesh networks as we could. Consequently, we consulted public and personal online resources, published proceedings of standards bodies, published books, as well as works-in progress and draft standards. We also attempted to model popular ad hoc schemes within the QualNet and

OPNet networking simulation and modeling tools. The main method of knowledge discovery, however, took place through our participation in NPS's Surveillance and Target Acquisition Network (STAN) series of experiments and our hands-on testing over the field experiments we conducted.

Data was collected by capturing salient network performance metrics, direct routing information contained within the nodes themselves, as well as generalized usability observations.

F. ORGANIZATION OF THESIS

The organization of this thesis is as follows:

Chapter II provides an overview of the routing protocols that are currently under active development or that hold the most promise from a militarily significant point of view. Additionally, it provides a description of the differences between wireless mesh networks and simple wireless ad hoc networks.

Chapter III examines the major categories of wireless mesh networks, what makes each different from the others and how they might be mixed and fused with other communications technologies to create a new communications paradigm for the future.

Chapter IV provides an overview of the various experiments conducted to examine the usability and efficacy of Layer 3, standards-based mesh networks.

Chapter V develops the idea of application layer mesh networking and outlines a high level, product-line architecture for a set of applications and the data interchange mechanism that could possibly enable ubiquitous network presence with the goal of information superiority.

Chapter VI provides some possible applications of wireless mesh networks for the Department of Defense's Global Information Grid. It provides some implementation recommendations with regard to planning considerations for deployment. Additionally, a concrete business case example is provided for a fixed mesh implementation.

Chapter VII includes our conclusions on the feasibility and applicability of IEEE 802.x wireless mesh networks within the Global Information Grid in light of the current state of technology. Recommendations for future research in this area are also included.

II. NETWORK LAYER WIRELESS MESH NETWORKING

A. MESH VS. SIMPLE AD HOC AND MANET

The authors have chosen to differentiate between wireless mesh networking and simple, wireless ad hoc networking in order to emphasize the specific issues that arise in network layer, multi-hop routing architectures where every node is a routing-capable node. The IEEE 802.11 standard provides for an "ad hoc" mode through the use of the Independent Basic Service Set (IBSS) paradigm that allows peer-to-peer functionality between end-use clients. These peering groups offer the advantage of quick configuration and rapid setup without the need for infrastructure access points, but there are limitations, as well. The primary issue is that full functionality and visibility amongst all peers is only possible as long as all members are within radio range of everyone else. No frame relay to members out of range of all other members is possible in an IBSS. Our focus was specifically on the ad hoc networks that incorporate routing at the node level and at layers higher than the physical and data link layers of the OSI model.

Additionally, we chose to avoid the term MANET, because of the limited scope of the Internet Engineering Task Force's MANET Working Group. While many of the militarily significant applications of wireless networking will require mobility and ad hoc formation characteristics, there are GIG segments that are essentially fixed that may derive benefit from a multi-hop, wireless solution framework. Hence, we will hereafter use mesh as the working term encompassing all aspects of self-forming, self-healing, multi-hop-routable networks.

B. DESIRABLE CHARACTERISTICS OF WIRELESS MESH NETWORKS

Simply from the standpoint of natural selection, wireless mesh networking must offer something better than current networking technologies for it to be considered the logical successor to traditional network models. There are several high-level characteristics of the mesh topology that, indeed, make this the case.

One of the characteristics of wireless mesh networks that make them attractive as a networking paradigm is the same element that makes the Internet viable. The ability to do peer-to-peer routing, as is the case within the backbone of the Internet, adds redundancy to the vital communication links from end-to-end. This added redundancy brings reliability and availability gains which, in a wireless network, are essential to effective operation at the edges.

One of the most important and unique hallmarks of wireless mesh networks is the concept of extendability. We will expand on the nature of extendability in later chapters, but the general theory is that nodes are no longer tied to fixed access points by the range of their own single radio. As more nodes are added, the reach of the mesh physically extends outward and, if nodes are added to the interior pathways, the mesh may even get stronger.

The concept of self-forming networks is also optimized through the mesh paradigm. While standard 802.11 ad hoc mode makes self-forming wireless networking a reality, when combined with the extendability aspect, meshes can form fractally, in an extended configuration from the outset. Every node will be responsible for forming and will be able to join the mesh as soon as it is powered up, given similar nodes around it.

Finally, the self-healing mechanism of meshes, related to both self-forming and redundancy traits, truly sets mesh apart as an enabler for the networked world of the future. By ensuring that as nodes drop out, routes are recalculated and logical gaps are bridged, a self-healing mesh moves toward end-to-end, always-on computing where the network is ever-present and ever-usable.

C. ROUTING ALGORITHM AND PROTOCOL OVERVIEW

Layer 3, multi-hop routing protocols can be divided into two general behavioral families: proactive and reactive. Additionally, there is an extensive set of hybrids and combinations of those two families that have been postulated or developed to mitigate the shortcomings of the traditional solutions. To keep the scope of our investigation manageable, we chose to concentrate on a few representative members from each general category. Additionally, the four protocols that have achieved the status of experimental Requests For Comments (RFC) by the Internet Engineering Task Force (IETF) (i.e. – AODV, DSR, OLSR and TBRPF) are among our choices.

1. Proactive Protocols

The hallmark of proactive routing protocols is that each node attempts to maintain routes to all reachable destinations at all times, regardless of that individual node's requirement to send data to those other destinations.[2] This shortest-path routing mechanism carries an attendant amount of overhead associated with the route maintenance task.

Our goal of investigating the most robust, well-researched, and militarily suitable proactive protocols led us to pare down the extensive list of all proposed and theorized mechanisms to just a handful that we felt warranted further examination.

a. OLSR

The Optimized Link State Routing (OLSR) protocol is a fairly mature, proactive protocol whose semantics are relatively easy to follow throughout the routing service. OLSR is table-driven and uses the link-state scheme in an optimized manner to diffuse topology information. It uses the same basic approach as a classic link-state algorithm in that the link-state information is flooded throughout the network. However, since the protocol runs in wireless multi-hop scenarios the message flooding in OLSR is optimized to preserve bandwidth. A technique called MultiPoint Relaying (MPR) is used for optimization of the message flooding, which seeks to reduce the number of duplicate retransmissions while forwarding a broadcast packet. A reduction in packet retransmission is achieved by restricting the set of nodes retransmitting packets from all nodes to a subset of all nodes dependent on the topology of the network.

OLSR operation mainly consists of updating and maintaining information in a variety of tables. Route calculation is derived from the information in the tables. The data in these tables is based on received control traffic. OLSR defines three basic types of control messages:

HELLO – HELLO messages are transmitted to all neighbors and are used for neighbor sensing and MPR calculation.

[2] R. Ogier and others, *Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)*. RFC 3684, Internet Engineering Task Force (IETF), February 2004, 4.

TC – Topology Control messages are the link state signaling done by OLSR, and are optimized in several ways using MPRs.

MID - Multiple Interface Declaration messages are transmitted by nodes running OLSR on more than one interface. These messages list all IP addresses used by a node.[3]

OLSR is currently available for several different hardware and operating system architectures.

b. MMRP

The Mobile Mesh Routing Protocol (MMRP) is actually a suite of three protocols developed by the MITRE Corporation as part of their Mobile Mesh project.[4] The three components of the suite manage link discovery, routing, and border discovery through loosely coupled programs that work together with a common data format and syntax.

Each of these protocols contains only a single message type, which makes them easy to understand. Additionally, by keeping each function separate, flexibility and extensibility are enhanced. For example, if a radio is able to discover links at the link layer, there would be no need to run the link discovery protocol—yet the routing protocol could still be utilized.

The three protocols are briefly described below:

Link Discovery

The Mobile Mesh Link Discovery Protocol (MMLDP) is based upon a traditional "HELLO" protocol. Periodically, a HELLO message is broadcast that contains the nodal interface address and the addresses of the interfaces that it has heard HELLO messages from previously.

[3] Andreas Tonnesen, "Implementing and Extending the Optimized Link State Routing Protocol" (UniK University Graduate Center, University of Oslo, 1 August 2004), 8.

[4] MITRE Corporation, *Our Work – Technology Tranfer – Mobile Mesh.* Last Updated 08 October 2003, http://www.mitre.org/work/tech_transfer/mobilemesh/, Last Accessed 9 September 2004.

Routing

The Mobile Mesh Routing Protocol is based on the link state approach. Each "Link State Packet" (LSP) contains various pieces of information including a unique router ID, a list that contains each local interface address, a list of neighbor interface addresses, and a list of "External Route Advertisements" which enable the node to advertise routes into the mobile cloud. Through External Route Advertisement, routers that have a wired connection to a fixed network can advertise a default route for mobile nodes, which enables mobile nodes to gain external connectivity.

Border Discovery

The Mobile Mesh Border Discovery Protocol (MMBDP) allows traffic flow existing outside the mobile cloud to be utilized. The basic premise is that if two or more nodes in the mobile cloud each have a connection into a fixed network (“border" routers), then the opportunity exists for mobile nodes to communicate with other mobile nodes across the fixed network. However, this protocol was not enabled in MMRP version used for our research.[5]

MMRP is available on both the Linux and Microsoft Windows operating systems and the application implementations interact between heterogeneous operating system nodes (e.g., a node running the Microsoft Windows version of MMRP will readily interact with a node running the Linux MMRP implementation).

c. TBRPF

Topology dissemination Based on Reverse-Path Forwarding (TBPRF) is another proactive protocol, but one that has optimizations built in to minimize some of the inherent, aforementioned drawbacks of proactive routing.

TBRPF consists of two modules: the neighbor discovery module, which performs topology discovery, and the routing module, which computes best routes.

Neighbor Discovery

The key feature of the TBRPF Neighbor Discovery (TND) protocol is that it uses "differential" HELLO messages which only report changes in the status of

[5] Ibid.

neighbors. Thus, HELLO messages are much smaller than those of other link-state routing protocols, which typically include the IDs of all neighbors. However, each node can optionally report additional topology information, up to the full topology, to provide improved robustness in highly mobile networks. One benefit of smaller HELLO messages is that they can be sent more frequently, which allows faster detection of topology changes. The result is that the protocol can quickly detect when a bidirectional link breaks or becomes unidirectional.

Routing Module

Each node maintains a source tree of shortest paths to all reachable nodes, but only reports a part of its source tree to its neighbors. Thus, overhead is minimized. This partial source tree report is sent to neighbors in periodic updates at a specified time interval (e.g., every five seconds), and a change report (additions and deletions) are sent in more frequent differential updates (e.g., every one second). Whenever possible, topology updates are included in the same packet as a HELLO message to minimize the number of control packets sent. Additionally, TBRPF does not require reliable or sequenced delivery of messages (e.g., no SYN-ACK is required), which further eliminates unnecessary network traffic and reduces overhead.[6]

An implementation of TBRPF is available commercially, only.

2. Reactive Protocols

As with the proactive family of protocols, after our initial literature research we pared down the list of all possible reactive mechanisms to a few that we felt warranted further examination.

The reactive routing scheme contrasts sharply with the proactive approach. Whereas the proactive protocols generally attempt to maintain an updated picture of the state of the entire network by continuously propagating routing information, the reactive, or on-demand, family seeks out routes only when there is data to be sent and routes are not known.

---

[6] Ogier, 3, 6-10.

a. DSR

The Dynamic Source Routing (DSR) protocol is a true on-demand protocol that limits its overhead to only that required to adjust to changes in path-in-use status. DSR is composed of Route Discovery and Route Maintenance mechanisms that work together to allow the discovery and maintenance of source routes in the ad hoc network. Both mechanisms operate entirely “on demand,” because each node keeps a “route cache” of all routes it has learned. Thus, no periodic updates of any kind are required once all routes are known, which drastically reduced overhead. For example, overhead packets could potentially scale all the way down to zero if all nodes were approximately stationary with respect to each other and all routes had been previously discovered. The technique of caching routes from Route Discovery broadcasts also serves to allow nodes multiple paths to other nodes, which results in rapid reaction to routing changes.

Route Discovery

Route Discovery is only initiated when a sending node determines it does not have a valid route to the destination address. In that case, the sender transmits a single, local “Route Request” packet to all nodes currently within wireless transmission range. Each Route Request contains a record of all the addresses of each intermediate node through which this copy of the Route Request has been forwarded. If the receiving node is not the destination address, the node appends its own address to the Route Request and rebroadcasts it. If the address of the receiving node is already listed in the Route Request, the packet is discarded. When the destination address is reached, the destination node will initiate a “Route Reply” back to the sending node, first examining its own route cache for a route back and if no route is found, initiating its own Route Discovery back to the original sending node.

Route Maintenance

Route Maintenance is the mechanism by which a node is able to detect if the network topology has changed such that it can no longer use a particular route to a specific node because a link along the route no longer works. When Route Maintenance indicates a source route is broken, another cached route is tried. If no other route to the destination address is known, the sending node initiates the Route Discovery mechanism again to find a new route to the destination.

DSR is unique in that both the Route Discovery and the Route Maintenance mechanisms allow support for unidirectional links and asymmetric routes to destination addresses. This is an important distinction; in wireless networks it is entirely possible that a link between two nodes might not work equally well in both directions due to propagation patterns or interference sources. In that case, support for unidirectional links could improve overall performance and network connectivity by allowing use of the best route in either direction.[7]

b. AODV

Designed for use in mobile ad hoc networks with populations of tens to thousands of mobile nodes, the Ad hoc On-demand Distance Vector routing protocol (AODV) can handle low, moderate, and relatively high mobility rates, as well as a variety of network traffic levels. It is designed to eliminate overhead on data traffic by reducing control traffic, thus scalability and performance are increased.

The message types defined by AODV include Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs).

Route Requests

A node broadcasts a RREQ when it determines that a route to a new destination is needed. A route is determined to be needed if the destination is unknown to the sending node, or if a previously valid route existed and then expires. The route is determined when the RREQ reaches either the destination address or any node with a valid route to the destination address.

Route Replies

A node generates a RREP back to the sender if either it is the destination or it has a valid, active route to the destination.

---

[7] David B. Johnson and others, *The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks.* Internet-Draft Work in Progress, IETF MANET Working Group, 15 April 2003, 1-2,4-10.

Route Errors

Link status of next hops in active routes is monitored by each node. If a break in an active route occurs, one or more destinations or subnets may become unreachable. If this happens, a RERR message is sent to other nodes indicating that a loss of link has occurred.[8]

AODV is available through a Java-based implementation, through an Intel Corporation-developed freeware program for Microsoft Windows, and from the National Institute of Standards and Technology (NIST) on the Linux operating system as a kernel modification.

3. Hybrid and Combination Protocols

Although some of the aforementioned routing protocols are well-suited to certain usage environments, there is no single "best" protocol that covers every conceivable scenario well. As a result, an entire genre of hybrid and combination protocols or protocol structures has been developed. Two of the most promising, from a GIG application standpoint, are the Zone Routing Protocol (ZRP) and the Landmark Ad Hoc Routing (LANMAR) protocol. The two protocols take different approaches in attempting to solve the shortcomings of the traditional methodologies.

a. ZRP

The Zone Routing Protocol attempts to break the network routing problem into a collection of smaller zones to maximize the efficiencies contained within both the proactive and reactive protocol families. ZRP acts as a protocol "framework" rather than a protocol in its own right.[9] The three components that make up the ZRP framework are the Intrazone Routing Protocol (IARP), the Interzone Routing Protocol (IERP), and the Bordercast Routing Protocol (BRP).

Although ZRP seems to behave hierarchically, it is actually "flat" in its implementation because there are no fixed clusters that use static clusterheads or master nodes. Each node defines its own zone size which is simply the number of hops to the

8 C. Perkins and others, *Ad Hoc On-Demand Distance Vector (AODV) Routing.* RFC 3561, Internet Engineering Task Force (IETF), July 2003, 2-4, 14-15, 18-19, 24-27.

9 Jan Schaumann, *Analysis of the Zone Routing Protocol* (08 December 2002). Electronic resource available from <http://www.netmeister.org/misc/zrp/zrp.pdf>, Last Accessed 09 Sep 04, 6.

edge of that particular zone. Any proactive protocol can be used within the zones (IARP) and nearly any reactive approach can be used in between zones (IERP).

There are no fixed nodes within the zone, so as the topology changes, so does the proactively built table of each and every node. Within the IARP zone, the knowledge of routes to other nodes is high, so latency can be expected to be low. External to the local zones, a reactive approach is used. Thus, within the IERP, there is little constant overhead because routes are only calculated on demand. To minimize looping and delay, however, a Bordercast Routing Protocol (BRP) algorithm exists that forms tree tables at the peripheral nodes to minimize redundant looks outside of the local zones.[10]

Interestingly, when the zone size is adjusted downward, ZRP essentially behaves in an almost purely reactive way by sending almost all traffic out of the local zone. In contrast, when the zone size parameter is increased, ZRP assumes the role of a proactive protocol. Although proponents of ZRP assert that it scales upward well, the fundamental fact that it deals with nodes on a largely individual level make latency and wide-ranging route management in a dynamic setting lingering question marks.

b. LANMAR

Another hybrid scheme has been developed that tries to overcome the disadvantages inherent in both the flat proactive and purely hierarchical protocols and that implements the best features of both. The Landmark Ad Hoc Routing protocol is predominantly a proactive protocol that uses the concept of logical groupings with dynamically elected "landmark" nodes to reduce hop counts between widely separated nodes in larger mesh networks.[11]

The protocol is an amalgamation of two complementary sub-protocols that cooperatively act to route data across the mesh. The first element is a purely proactive, table-driven protocol that is present at the common node level and which attempts to keep routing information current within a limited-hop scope. The second element is a higher-level, distance vector scheme that disseminates data about the dynamically elected

---

[10] Ibid, 10.

[11] K. Xu and others, "Landmark Routing in Large Wireless Battlefield Networks Using UAVs," in *Proceedings of IEEE MILCOM 2001*, 2001, 1.

landmark node within each logical grouping to the network at large.[12] Both mechanisms use the concept of myopic, Fisheye State Routing (FSR) between the nodes of interest. Similar to a fish's sight profile, nodes farther away tend to drop out of visibility and are no longer considered as part of the active cluster. One of the other basic tenets of basic LANMAR is that mobility will be mainly as a group and the clusters will remain relatively stable. This enhances the effectiveness of the FSR and the landmark concept by not having wildly changing topologies making individual nodes difficult to "find."

The clustering scheme that contains the landmarks is similar to logical subnetting. Each node has detailed local information about other nodes within its own FSR scope and distance vector routes to all the other landmarks.[13] If a node needs to send a packet to a destination outside of its own limited cluster scope, it uses its distance vector table to get the packet toward the cluster landmark of the destination node. Inside the last cluster, the packet will be routed via its own local neighbors.

The theory behind LANMAR has been extended to include variations that maximize physical hierarchies with multiple radios (Hierarchical LANMAR), accommodate slightly higher mobility situations (Mobility LANMAR), as well as optimization for multicast environments (Multicast LANMAR).

4. Routing Protocol Summary

The seven protocols we chose to focus on in our research are highly representative of the most commonly found theories and implementations within the wireless mesh and mobile ad hoc fields of study. Even though there is no single, ideal protocol solution for military applications, we believe a hybrid or composite mechanism, such as LANMAR, may be the most flexible and easily adaptable given the diverse range of employment scenarios and mixture of equipment that will be included in the network.

The summary table below provides a general, side-by-side overview of some of the salient characteristics of the protocols we focused on.

---

[12] M. Gerla and others, "Exploiting Mobility in Large Scale Ad Hoc Wireless Networks," *IEEE Computer Communication Workshop*, Dana Point, CA, 2003, 4-5.

[13] K. Xu and others, "Landmark Routing in Ad Hoc Networks with Mobile Backbones," *Journal of Parallel and Distributed Computing* 63, Issue 2 (February 2003): 15.

Protocol	Family	Theoretical vs. Implemented	Platform Availability
OLSR	Proactive	Implemented Gateway functionality limited in version available for MS Windows	Linux, Linux-based Handheld, MS Windows, Windows CE
MMRP	Proactive	Implemented Gateway functionality limited in version available for MS Windows	Linux, MS Windows
TBRPF	Proactive	Implemented commercially	
DSR	Reactive	Implemented but in pre-Alpha form	BSD Linux
AODV	Reactive	Implemented Gateway functionality limited in version available for MS Windows	Java, MS Windows, Linux
ZRP	True Hybrid	Theoretical	
LANMAR	Proactive/ Hierarchical	Research Implementation	Linux

Table 1. Routing Protocol Summary Table

There is an extensive collection of protocols we did not have an opportunity to examine or evaluate. A graphical depiction of the current "universe" of protocols is contained in the figure below.

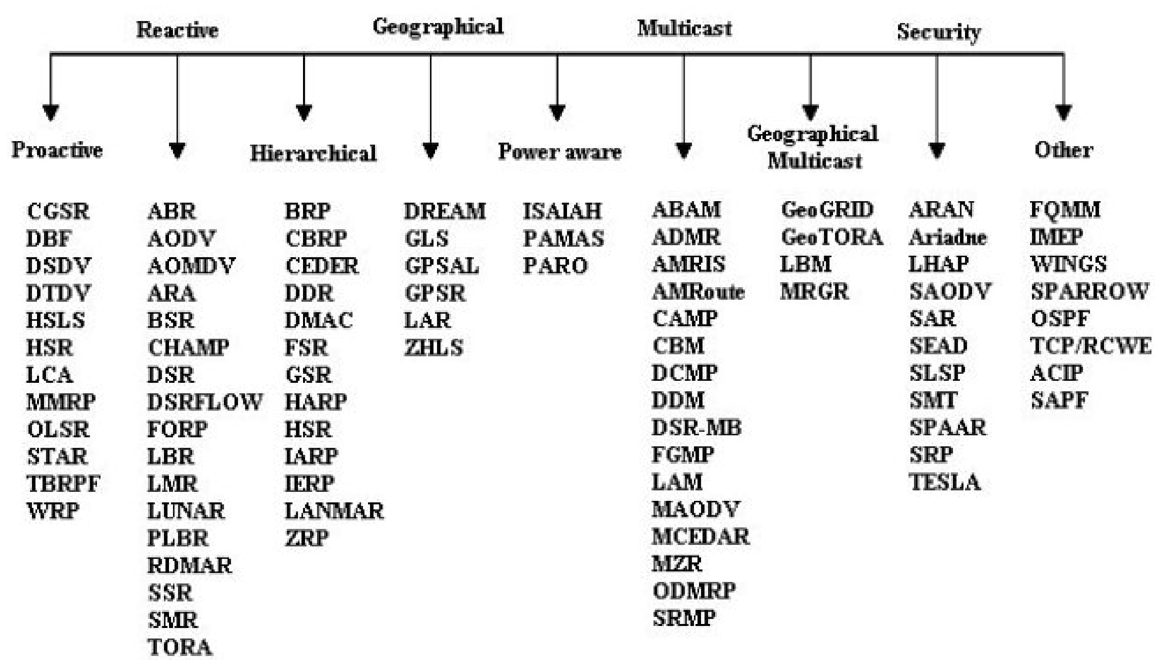


Figure 1. Collection of Known Ad Hoc Routing Protocols (From Halvardsson and Lindberg)[14]

[14] Mattias Halvardsson and Patrik Lindberg, "Reliable Group Communication in a Military Mobile Ad hoc Network" (Master's Thesis, Vaxjo University, February 2004), 15.

III. DETAILED ANALYSIS OF MESH ARCHITECTURES

A. FIXED

While trying to differentiate types of mesh architectures from one another, we decided on the category of "fixed" for mesh networks that leverage the static, physical infrastructure as the main schema for distributing their nodes. The characteristic most often associated with fixed wireless mesh is the mesh-enabled access point. Providers most often implement mesh algorithms at the access point level, but leave client nodes in a non-meshed state.

Traditionally, the most costly and time-consuming piece of corporate/community wireless networking implementations is the placement and continued usage fees associated with high-speed backhaul paths. Secondarily, the point-to-multi-point wireless solution requires greater monitoring because of the inherent "single points of failure" that are created at the communal access points. These two elements, when coupled with the ease-of-setup and extendable nature of mesh access points make standards-based, fixed meshes an attractive alternative to the traditional wireless paradigm.

1. Mesh as a Backhaul Utility (IEEE 802.11 and 802.16)

As of this writing, current wireless networking standards and commercial ventures that deal in mesh are primarily focused on the use of mesh as a backhaul technology to the wired Internet. The proverbial "last mile" of broadband network access to consumers is increasingly being bridged by wireless solutions, and Wireless Internet Service Providers (WISPs) are beginning to turn to mesh technologies as a way to fulfill their need for easily deployable access points. Hotspots, with communal wireless access points, are also considered here as part of the backhaul to the wired world.

a. Community Wireless Projects

Large-scale examples of fixed mesh architectures that use three separate mesh networking technologies include community wireless projects such as WiFi Hermosa Beach, the city of Cerritos, California, and the Stevenson Wi-Fi Project. Although based on different proprietary mesh technologies, all three projects serve as good examples of how communities are solving the problem of providing widespread wireless access to their residents and guests through the most cost-effective means available. A graphical depiction of one version of a community mesh is included below. These projects use multi-hop, meshed access points to provide the broadband backhaul to the wired Internet. The end-user nodes are typically standard 802.11 clients that use the meshed access points the same way as standard infrastructure-based wireless operates, with packets funneled to "supernodes" that bridge the wireless and the wired networks.

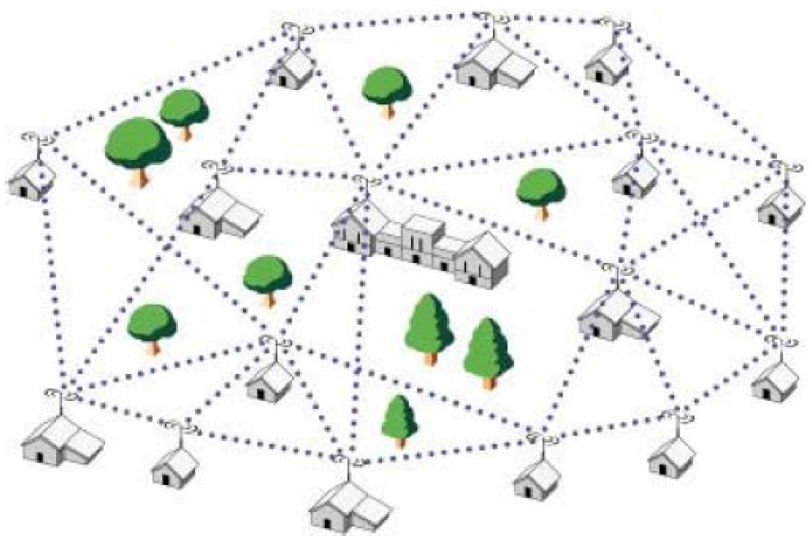


Figure 2. Community Mesh Example (From Nokia 802.16a Tutorial)[15]

b. Current Commercial Solutions

There are presently several commercial mesh networking equipment providers that are offering community and business solutions. While the scope of this thesis is geared toward non-proprietary, open standards, the efforts of several commercial companies are built on a standards-compliant technology base and merit mention.

The technology that the Hermosa Beach, California, network is built on is from Strix Systems of Calabasas, California. Their solution, the "Access/One Network," uses modular, multiple radios in different 802.11 configurations to separate the task of mesh backhaul from that of a client access point. This offloads much of the overhead that would degrade performance on a single radio solution. To effectively mesh, Strix

[15] Dave Beyer and others, *802.16 Mesh Extensions – Overview*, <http://www.ieee802.org/16/tga/contrib/S80216a-02_30.pdf>, March 2002, Last Accessed 29 Aug 04, 2.

uses a proprietary algorithm that constantly polls for routing and node health data to optimize the best paths.[16] Their modular hardware is displayed in the figure below.

Figure 3. Size Illustration of Strix Network/One Modules (From Strix Systems Website)[17]

The Cerritos mesh uses equipment from Tropos Networks of Sunnyvale, California. They use their own Predictive Wireless Routing Protocol (PWRP) with a single radio to serve as both access point to one-to-many clients and as a mesh routing node amongst one-to-many access points. Wired backhaul connections are integral to maintaining the viability of this architecture, especially when the number of nodes begins to grow. The configuration of their "Tropos Sphere," composed of something they term "Wi-Fi cells," is displayed below.[18]

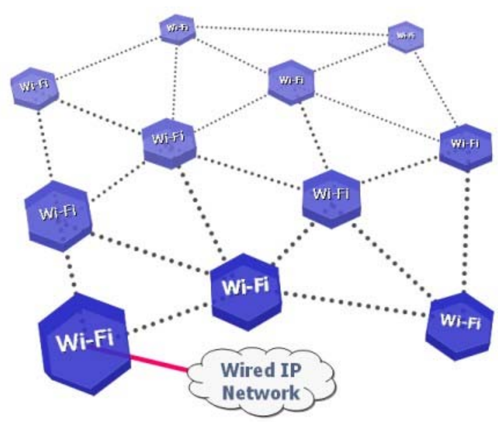


Figure 4. Tropos Networks' Tropos Sphere (From Tropos Networks Website)[19]

[16] Strix Systems, "Access/One Network Product Description," <http://www.strixsystems.com/downloads/product_description/Strix_prodescription_web.pdf>, Last Accessed 02 Sep 04, 4.

[17] Strix Systems, "Products," <http://www.strixsystems.com/products/products_main.asp>, Last Accessed 03 Sep 04.

[18] Tropos Networks, "Technology," < http://www.tropos.com/technology/>, Last Accessed 03 Sep 04.

[19] Ibid.

Lastly, the Stevenson Wi-Fi Project in Stevenson, Washington, uses LocustWorld as their technology provider. LocustWorld is a company from the United Kingdom that has taken the Ad hoc On-Demand Distance Vector routing protocol from the U.S. National Institute of Standards and Technology (NIST) and included it inside a software package, MeshAP, which provides management features to optimize mesh behavior and provide security. Their solution is composed almost entirely of open source and standards-based components, yet seems to scale well in the communities in which it has been adopted.[20]

One of the major debates within the mesh world, besides the search for the best routing protocol, centers on the efficiency to be gained from using multiple radios versus a single one. The commercial providers have evenly split on that question; especially as new algorithmic mechanisms emerge to minimize the bandwidth degradation attendant with the single radio option. Even though differences exist on methods of implementation, there is clearly a great deal of momentum building from the commercial fixed mesh sector that will be hard for the DoD to ignore in the not-too-distant future.

c. Emerging Standards Base

The two biggest emerging segments of wireless backhaul and hotspots for WISPs are 802.11b/g and 802.16 draft technologies. Within both the 802.11 and 802.16 worlds, there are budding standards that include meshability as an extension of the standard modes of operation. These emerging standards may go a long way toward making the promise of widespread mesh plausible in the near term.

IEEE 802.11s is emerging as an extension to the 802.11 MAC layer specification which delineates mesh configuration and forwarding at Layer 2 for up to thirty-two access point nodes. The proposed "Extended Service Set (ESS) Mesh" would create a "Wireless Distribution System (WDS)" that accommodates broadcast/multicast as well as unicast communications between the multi-hop routable, meshed access points. Interestingly, this proposed standard allows for the use of multiple radios within the individual access points, so the standard will not settle the internal debate on that point.

[20] LocustWorld, "The Information Revolution – Mesh Networking Hardware and Software," <http://locustworld.com/index.php>, Last Accessed 03 Sep 04.

The Project Authorization Request (PAR) delineates an expected completion date for the standard of 01 January 2007.[21]

The IEEE 802.16 Mesh Ad Hoc Committee has a proposed approach to lower-layer mesh that is a bit different and more robust than the approach taken by the 802.11s group. Their mesh involves clustering and is very similar to the zone routing mechanism outlined in Chapter II. They propose the concept of clusters of “AirHoods” that have an “AirHead” that forwards and controls traffic bound for other “AirHoods” or the backhaul path to a wireline network.[22] The standard will most likely be designated 802.16f and is expected to be quickly adopted once 802.16 becomes a more widely accepted standard in its own right. For a more detailed examination of the role of 802.16 within the DoD, see Ryan Blazevich’s Naval Postgraduate School Master’s Thesis entitled, “Wireless, Long Haul, Multi-Path Networking: Transforming Fleet Tactical Network Operations With Rapidly Deployable, Composable, Adaptive, Multi-Path Networking In Austere Environments.” (Sep 04)

2. A Generic Business Case for Fixed Mesh

Aside from the novelty and convenience of transitioning to a fixed, mesh access point network configuration, there is evidence that the total cost of ownership for the same data throughput is much lower than traditional wireless solutions.

Nortel Networks researched a real-world scenario, using downtown Toronto, Canada, as a business case illustrating a comparison of the Total Cost of Ownership (TCO) of traditional wireless hotspots versus a wireless mesh network. The following are the results of their research.

[21] Jim Hauser and others, *Draft PAR for IEEE 802.11 ESS Mesh* (14 November 2003), 6.

[22] Beyer, 4.

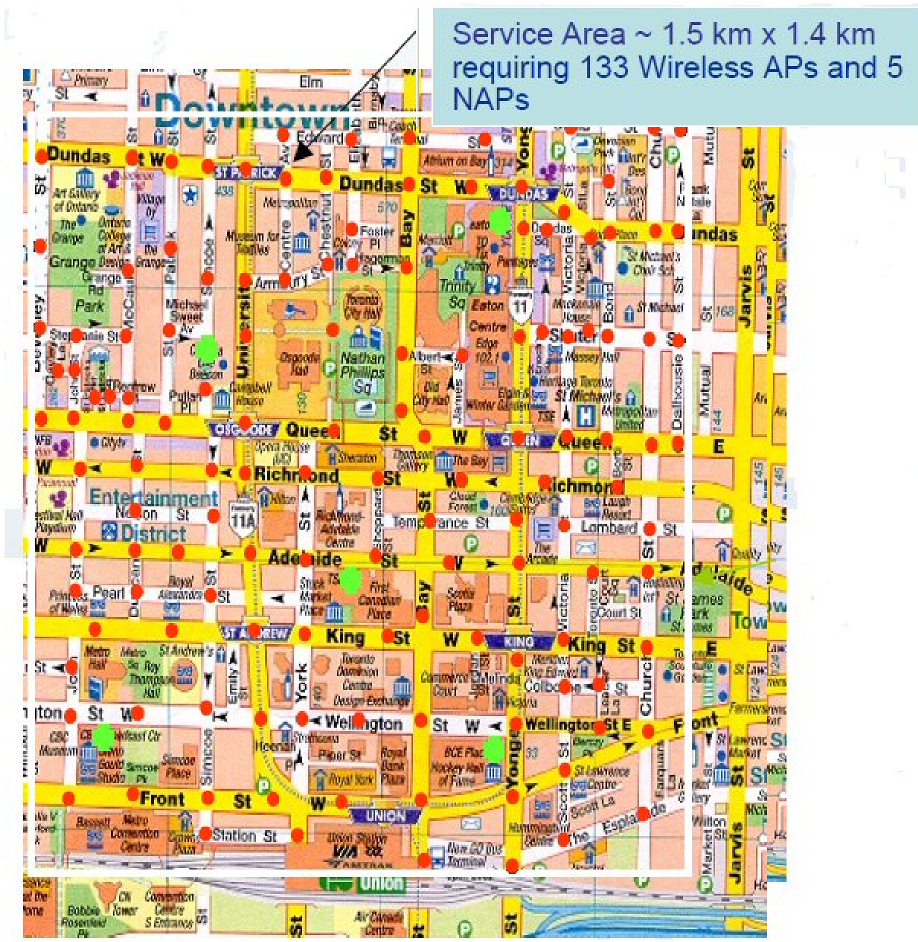


Figure 5. Downtown Toronto Service Area Considered in TCO Study (From Nortel Case)[23]

Situation:

- Study covered downtown Toronto (see figure), a dense urban area including financial, shopping, entertainment and government centers.
- Today, with a traditional wireless topology, only spotty hotspot coverage exists.
- With fixed wireless mesh, a complete, high capacity (200 Mbps), low cost data service throughput area is created.

Benefits:

- Lower operating expenses result from eliminating multiple T1 lines and replacing them with fewer T3 lines.

[23] Melissa Chee, *The Business Case for Wireless Mesh Networks* (11 December 2003). Electronic presentation available from <http://www.nortelnetworks.com/corporate/events/2003d/wmn_eseminar/>, Last Accessed 05 Sep 04, 10.

- Deployment is simplified by having fewer connections to make and maintain.

First Year Costs	Hotspots	Wireless Mesh Network
Installation - 133 APs & 133 T1s for hot spots - 133 Wireless APs, 5 NAPs & 5 T3s for Wireless Mesh Network - Assumptions: 4 hours/T1, 12 hours/T3, 1 hour/AP, 30 minutes/Wireless AP,1 hour/NAP, $50/hour	**$33,250**	**$6,575**
Backhaul - Hot Spot: T1 lease costs @ $500/T1/month - Wireless Mesh Network: T3 lease costs @ $4,000/T3/month	**$798,000**	**$240,000**
Total first year expense – backhaul & installation	**$831,250**	**$246,575**

Table 2. Business Case for Wireless Mesh Networks vs. Wireless Hotspots

As illustrated in this example, a traditional wireless hotspot solution requires 133 Access Points and 133 T1 data lines with a total first year expense (including installation) of $831,250. However, when a wireless mesh solution is applied to this problem, 133 Wireless Mesh Access Points are needed, but only five Network Access Points (NAPs) and five T3 phone lines. This results in a first year total cost (including installation) of just $246,575. In this example, using a fixed wireless mesh solution achieves cost savings of nearly $585,000, making it less than a third as expensive as the traditional solution.[24]

3. Fixed Mesh GIG Applicability

Within the Department of Defense and throughout the customer-base of the GIG, the amount of the enterprise that relies on information systems continues to rapidly increase. This reliance has also brought with it a desire for ubiquitous connectivity to access those information systems. The benefits of wireless networking begin to emerge

[24] Ibid, 10-11.

as workers use mobile devices inside the organization to stay “connected” at all times. A fixed mesh architecture to maximize information coverage while minimizing investment is an ideal fit.

Rapidly deployable and reconfigurable, fixed wireless networks can be erected in tactical operations centers and tent cities to keep information exchange flowing on or near the modern battlefield. Networks that can be “dropped in” with minimal setup time will become increasingly in demand as non-traditional missions continue to proliferate and standard headquarters elements are moved from the rear areas and scattered throughout the battlespace. Backhaul functionality will be integral to moving the situational awareness picture through the conflict continuum from the warfighting elements to the more static, geographically dispersed command echelons.

In addition to the tactical and operational level usage, we also foresee use of mesh solutions at existing stateside bases as an alternative to the costly traditional wired network paradigms that currently exist and are multiplying as computing commoditization continues. Based on the rough Total Cost of Ownership example above, broadband, base-wide mesh networks may become the model for the DoD enterprise when embarking on new network initiatives. For the GIG, the flexibility that fixed mesh networks provide makes the idea more than worthy of continued research and exploration.

B. MOBILE

One of the most compelling reasons to even consider a mesh networking solution is the potential benefit to be gained from the ability to be simultaneously mobile and networked. While fixed meshes may be a good first step in unwiring the “last mile” to end users, the promise of mobility is what may carry the multi-hop movement to near-ubiquity.

1. Usable COTS Framework (802.11)

The IEEE 802.11 specification is the most well-known and integrated COTS wireless networking standard on the market, today. The momentum created by 802.11b, and now 802.11g, technology has made wireless computing a reality for tens of thousands of consumer and business users. The 802.11b/g combination has made great strides in penetrating the portable computing market as a ubiquitous accessory. It is now commonplace for consumers to have to de-select the option of included wireless when purchasing new portable computing devices.

Within the end-user space of 802.11, there seems to be a groundswell building toward even more mobility than is currently the norm. When contrasted with the range and mobility of cellular telephony, traditional access point-based wireless solutions entail a short-range tether that is becoming a true limiter for consumer-level adoption. The only way to overcome the perceived short range and tether issues associated with the hub-and-spoke model is to either make many more hubs by seeding additional access points, or by extending and interlacing the end-user framework. Both of these options are realizable with mesh, and the latter path is the cutting edge of mesh research, today.

2. Mesh Elasticity

One of the primary motivations for mobile meshes is the expandability and flexibility that routing in each node brings. While in simple ad hoc mode, complete communication paths can only be maintained as long as all nodes are within radio range of all other nodes. We used a simple geometric expansion theory of

$$E = (n-1)*d$$

Where:

E = expansion distance

n = number of peering nodes

d = effective radio range

This is subject to propagation, noise, interference and other losses. Using this equation as a general rule of thumb, mobile meshes are able to extend outward much farther than what is possible in traditional, infrastructure-based or ad hoc-based 802.11 wireless, as illustrated in the figure below.

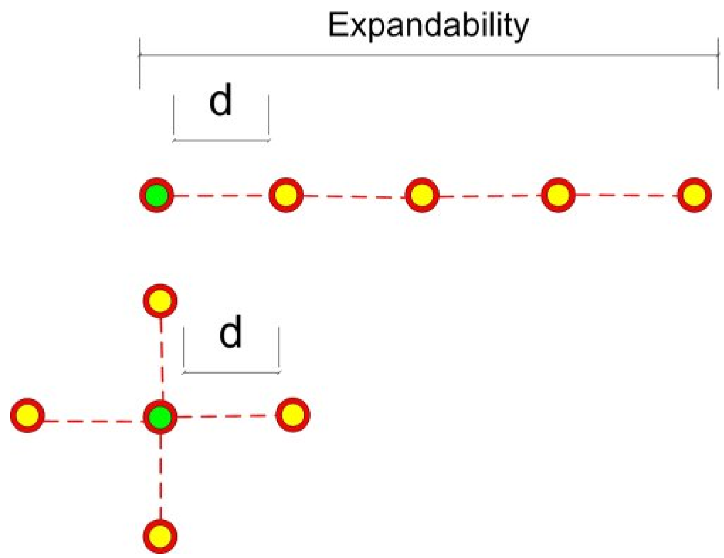


Figure 6. Range Comparison of Mesh (top) vs. Traditional Wireless (bottom)

This expansion possibility makes the mesh construct the potential “killer enabler” for personal communications of the future. As soon as end-users are willing to provide computing power for the routing of other nodes’ traffic, adoption of mobile meshes may skyrocket. For example, today there are still wide lapses in cellular network coverage, especially in open, less densely populated areas. Once the engineering and social issues are resolved, the combination of fixed and mobile meshes could fill gaps and provide reach to countless individuals at much higher data rates than cell phones currently provide.

3. Effects of Node Mobility

Mobile nodes are both a liability and strength to mobile mesh networks. While node mobility often brings the undesirable effect of rapid changes in network topology, broken routes, and configuration overhead, there are some benefits to be gained, as well. Mobile nodes that wander into sparsely populated clusters serve to provide one more hop that strengthens the fabric of the mesh. The routing power that is donated to the cluster may far exceed the cost of topology control traffic that is generated by the new node.

Predictive, geospatially-aware routing and intelligent backhaul mechanisms could direct data through the best routes at the best times in order to optimize the state of the entire network. These issues will be addressed further in our treatment of potential application layer mesh approaches and in Chapter VI.

4. Mobile Mesh GIG Applicability

The centerpiece of the GIG is the concept of the fully-networked warrior. Within the Department of Defense, the roots of wireless mobile mesh networking extend back over three decades. The Defense Advanced Research Projects Agency (DARPA) was one of the first entities to sponsor research into workable solutions for multi-hop wireless networks. One of the latest results of the decades of research and experimentation is the U.S. Army's Land Warrior Program, which represents the vision of integrating the individual infantry soldier into a digitally-enhanced battlefield. One aspect of Land Warrior includes a wearable computer and wireless communications package that connects the warrior to everything else within the battlespace for maximum situational awareness.[25]

The success of initiatives like Land Warrior will be dependent on a robust, mobile mesh backbone. Given the direction of recent research and advancements in the field, wireless mesh may become the true enabler of the mobile, networked battleforce. The GIG may seek to be an end-to-end solution, but the mobile segment is the most vital, difficult and potentially rewarding segment of that continuum.

C. SENSOR

Architectures comprised of low data rate, long-lived sensors comprise the simplest segment of the mesh networking spectrum. While essentially a different technology approach at the PHY and MAC layers from that of 802.11 or 802.16, the sensor standardization effort, under the 802.15.4 umbrella, is growing in importance on several levels.

1. Low Data Rate Solutions (IEEE 802.15.4/ZigBee)

While examining fixed and mobile meshes we have largely covered traditional Layer 3 (IP packet) routing, the WPAN mesh solution focuses on a simplified, hierarchical, and optimized table-driven approach that minimizes complexity and leverages the typical deployment theory behind sensor nets. While the 802.15.4 standard

[25] Exponent Corporation, "Land Warrior Program," <http://www.exponent.com/practices/techdev/landwarrior/index.html>, Last Accessed 06 Sep 04.

addresses the physical and MAC layers, the specialized ZigBee network layer exists primarily to accommodate the routing functionality required to fully mesh the sensors together.[26]

2. Aggregation and Integration Issues

Sensor information that is relayed over the multi-hop mesh usually needs further processing before it is able to be used by human monitors. While scalable to many sensor nodes, data is not passed into a larger, IP-based network directly from any edge sensor but is collected and translated via some intelligent aggregation point that is running a higher-level operating system and which has more computing power at its disposal. Typically, the aggregation point acts as both a data parser and a bridge to some larger network segment. The data frames that arrive at the aggregation points must be processed, somehow, to enable seamless integration and interoperability throughout the rest of the network.

a. Current Commercial Solutions

As with the fixed wireless mesh world, there are commercial entities that are beginning to emerge as solutions providers within the sensor mesh realm of operations. Again, although our research is concerned with the development of the 802.x standards-compliant technologies, the commercial entities presented here represent the most readily available, viable solutions derived from those standards.

Ember Corporation, of Boston, Massachusetts, provides low date rate sensors that are specifically geared towards sensing and control applications. Their proprietary EmberNet Protocol Stack contains their routing mechanism and resides on each of the microprocessors that make up the sensor mesh. Their aggregation points run Ember Studio, a software application that displays node data and also allows network control and management.[27]

---

[26] Patrick Kinney, “ZigBee Technology: Wireless Control that Simply Works,” *Communications Design Conference*, October 2003, <http://www.zigbee.org/resources/documents/ZigBee_Technology_Sept2003.doc>, Last Accessed 08 September 2004, 14.

[27] Ember Corporation, “Ember Product Family,” <http://www.ember.com/products/family/index.html>, Last Accessed 05 Sep 04.

Crossbow Technology, of San Jose, California, is one of the first companies to develop meshed sensors based on an open-source software base. Their SmartDust products use the open-source TinyOS to handle the processing and meshing features within the sensors. Their aggregation software also leverages third-party and open-source initiatives that provide monitoring and node health information views into the mesh.[28]

As in both the fixed and mobile mesh categories, there are differences in the approaches of many of the entrants into the field of sensor mesh networking, but the underlying goal of creating robust, lightweight networks remains a constant.

b. SensorML

Within the sensor mesh world, work has already begun on a data interchange mechanism and Extensible Markup Language (XML) vocabulary that allows much more efficient parsing of sensor-unique data. The approach that is gaining ground is known as Sensor Modeling Language (SensorML).[29] SensorML describes and provides a mechanism for definition of the various properties of sensors and the data that comprises their output. It is, a "schema for defining the geometric, dynamic, and observational characteristics of a sensor."[30] By dealing at just the level of the frame payload, SensorML is compact yet scalable and is immune to the restrictions of traditional Internet Protocol packet formatting. SensorML also contains provisions for geo-description of sensor nodes as well as capability advertisement through part of its schema information.

The Uniform Modeling Language (UML) model for the basic decomposition of the abstract components of SensorML is shown below. The model is intriguing because the basic attributes are placeholders for the XML data within each component. By using SensorML, each sensor or collection of sensors is able to fully describe its identity, where it is, what it can do, and how it fits into a larger topology.

---

[28] Crossbow Technology, *Motes, SmartDust Sensors, Wireless Sensor Networks,* <http://www.xbow.com/Products/productsdetails.aspx?sid=3>, Last Accessed 05 Sep 04.

[29] "Sensor Model Language (SensorML)," February 26, 2004. <http://vast.uah.edu/SensorML/>, Last Accessed 13 August 2004.

[30] Mike Botts, *Sensor Model Language (SensorML) Version 0.6*. Electronic presentation available from <http://vast.nsstc.uah.edu/SensorML/SensorML.ppt>, Last Accessed 04 Sep 04, 6.

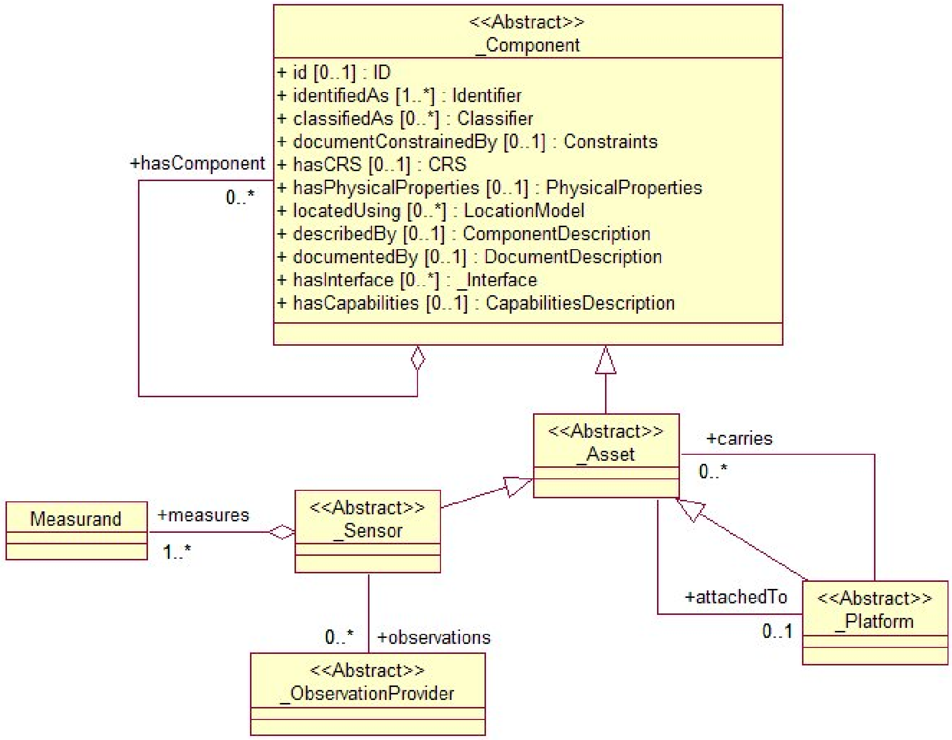


Figure 7. UML Model of SensorML Components (From SenorML Models Paper)[31]

3. Sensor Mesh GIG Applicability

The maturity and fast-paced evolution of low data rate, long-lived sensor mesh technologies are two reasons why it is fast gaining ground within DoD, network-centric solution architectures. The sensor-to-shooter continuum often starts with unattended ground sensors that provide early indications and warnings to the forces in the field or higher echelons of command. However, because of the limited processing power within the sensors themselves the aggregation points become essential to current implementations of sensor meshes. Unfortunately, they present the problem of a single point of failure that, if exploited, could debilitate or degrade the entire mesh. Fortunately, as computing power continues to move down the miniaturization path, the robustness and computational richness of the sensors may increase enough to enable scalability and reachback without the tie to a vulnerable quasi-local aggregator.

31 Mike Botts, *Overview of the SensorML UML Models*. Unpublished draft available from <http://vast.nsstc.uah.edu/SensorML/SensorML_UML.doc>, Last Accessed 05 Sep 04, 1.

Fully meshing the sensor grid will pay huge dividends as solutions to aggregation and the ability to leverage sensor capabilities over the mesh begin to emerge and continue to develop.

D. HYBRID/MIXED MODE

An ideal scenario from a public safety or battlefield point of view would be to have all three mesh technologies integrate, seamlessly, over the network. Aggregation and translation mechanisms may slightly add to network latency, but a well-engineered solution could avert many of the issues of data compatibility. One such solution was achieved over our testbed during the course of our study. As illustrated in the figure below, we successfully integrated a 900 MHz sensor mesh into an 802.11b mobile mesh, then into a static 802.3 wireline network, back out through a draft 802.16 wireless link, through an abbreviated 802.16/802.3 stub and into another 802.11b mobile mesh where data from the sensors was presented (on node 210 in the illustration) after it had been processed on one of the servers (node 155) in the 802.3 loop.

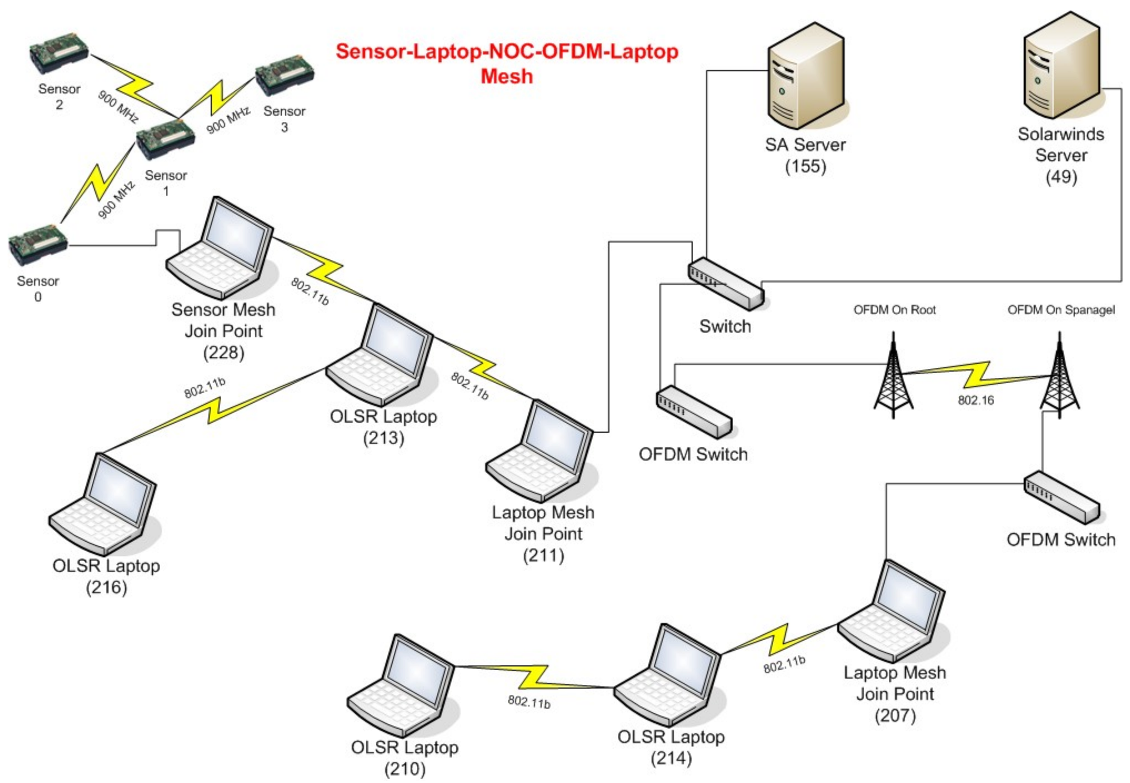


Figure 8. Multiple Mesh Segment Mixing

By combining the segments of the heterogeneous meshes, as outlined above and in Chapter IV, end-to-end situational awareness suddenly becomes an achievable goal. The biggest difficulty in any mesh combination for the foreseeable future will remain the routing methodology. Derived from our experience with the routing (OLSR) inside the multi-segment meshes we erected, and based upon the scenarios and simulation results contained within the literature, the LANMAR scheme seems well-suited to providing a traversal mechanism up and down the hierarchy of complex node types.

E. FUSION OF MESH WITH OTHER PARADIGMS

Even with effective integration of the 802.x-based mesh technologies, there exist many more opportunities for expansion and widespread usability. At the lower OSI layers, seamless mesh integration with the existing worldwide cellular systems and backhaul of localized meshes over satellite links is becoming a more likely possibility in the near term. The Motorola Corporation is now producing a handset that allows for Voice over Internet Protocol (VoIP) and cellular seamless roaming.[32] The device is intended for the corporate environment where localized VoIP exchanges are beginning to appear, but the technological leap is not far to accommodate a wider base of use.

As the standards within the 802.11, 802.15 and 802.16 families become solidified and mature, even more research and investment will be made to fuse all mesh and other communication mechanisms together. Two technologies that are gaining popularity and may have a place in the realization of heterogeneous communication fusion are Mobile Internet Protocol (MobileIP) and Mobile Access Routing.

1. Mobile IP and Address Autoconfiguration

One of the biggest technical challenges facing the effort to amalgamate wireless networks with cellular networks is the idea of address autoconfiguration. Mobile Internet Protocol initiatives seek to make addressing as transparent as possible across the network. In order to maintain a coherent "place" on the network, MobileIP uses the idea of "home addresses" and "care-of addresses" for end-user, mobile nodes. "Home agents" are responsible for maintaining addressing information for nodes that leave and register their

[32] Motorola, Inc., "Motorola Turns Enterprise Business Communications Inside Out," Motorola press release, 27 July 2004, <http://www.motorola.com/mediacenter/news/detail/0,,4493_3826_23,00.html>, Last Accessed 15 Aug 04.

care-of addresses on a “foreign network” via a “foreign agent.” Once a node registers itself on the foreign network, data can be encapsulated and transferred just as if the node was on its home network. The discovery, registration and tunneling process that occurs ensures end-to-end connectivity and usability across different network segments, but currently requires a well-known routing path between those segments.[33]

Address autoconfiguration, an idea that is built into Internet Protocol Version 6 (IPv6), may provide another method of easily identifying and tracking nodes between and across disparate sub-networks. IPv6 defines a method for nodes to statelessly set up a link local, site local and globally unique address as soon as they connect to the larger networking environment.[34] This may one day enable every node to simply establish itself within the global mesh, and immediately become a participant.

2. Mobile Access Routing Mechanisms

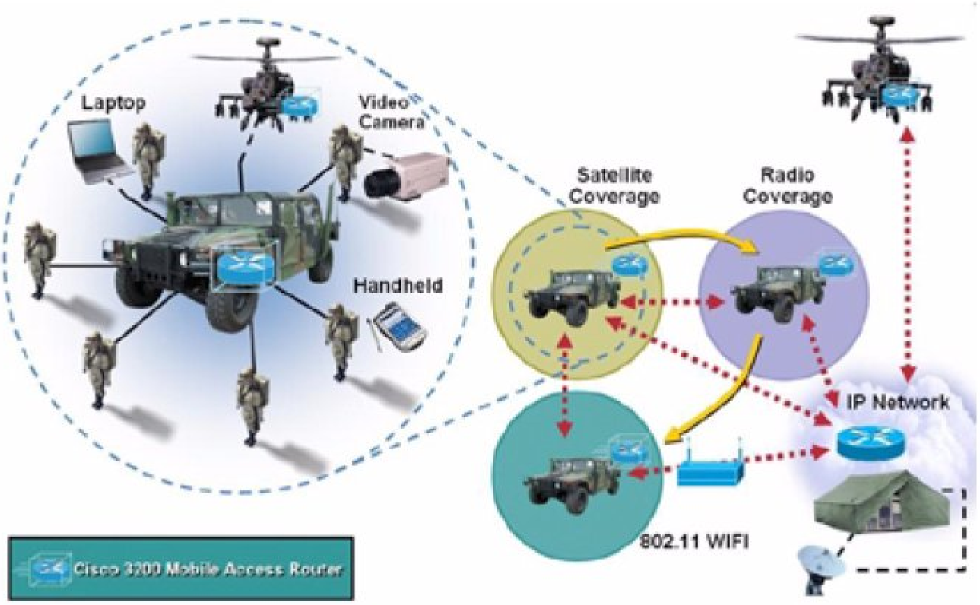
The other major technological hurdle to realizing full heterogeneous fusion is the challenge of reconfiguring and rerouting amongst different physical and link layer technologies. Even if address portability is achieved through one of the methods outlined above, seamless roaming that does not jeopardize usability is another matter altogether.

Current work on mobile access routing, to allow optimum network path choices to be made automatically, based on link strength, is still in its early stages but is being led by Cisco Systems. By combining MobileIP with link-aware routing, the Cisco Mobile Access Router (MAR) will attempt to provide constant connectivity over a variety of different backhaul paths.[35] An illustration of one possible DoD application for the MAR is included in the figure below.

[33] Charles E. Perkins, “Tutorial: MobileIP,” 1997, <http://www.computer.org/internet/v2n1/perkins.htm>, Last Accessed 06 Sep 04.

[34] S. Thomson and others, *IPv6 Stateless Address Autoconfiguration*. RFC 1971, Internet Engineering Task Force (IETF), August 1996, 3.

[35] Cisco Systems, “Cisco 3200 Series Wireless and Mobile Routers.” Electronic brochure available at < http://www.cisco.com/en/US/products/hw/routers/ps272/prod_brochure_list.html>, Last Accessed 06 Sep 04, 1.



Cisco 3200 Mobile Access Router Employment Example (From Cisco Systems)[36]

[36] Ibid, 2.

IV. EXPERIMENTATION AND RESULTS

A. OVERARCHING EXPERIMENTAL GOALS AND APPROACHES

Our mesh experimentation fell into three broad categories of formal experiments in a wider network context, less formal protocol examination and comparison work, and very preliminary work on application-level issues. Within that framework, we attempted to gather data points which would further clarify the problem space in which we were operating and which would give us a solid theoretical basis from which to draw preliminary conclusions about functionality and efficacy.

B. SURVEILLANCE AND TARGET ACQUISITION NETWORK EXPERIMENT SIX (STAN 6)

NPS's Surveillance and Target Acquisition Network Experiment Six (STAN 6) was conducted May 1-6, 2004, at Camp Roberts in California. This sixth iteration of the quarterly recurring series of field experiments had as its high-level goals a collection of networking interoperability tasks across multiple hardware segments to establish and improve situational awareness on the battlefield. One of the secondary goals was to prove that COTS wireless mesh networking technologies merited further examination within the DoD research community.

C. STAN 6 EXPERIMENTAL OBJECTIVES

Within the larger STAN framework, the multi-hop, mobile ad hoc networking experimental objectives encompassed five separate spheres of investigation.

1. Compare/Contrast Different Routing Protocols

A detailed comparison of the most well-known, readily available ad hoc routing protocols was one of the primary objectives of the experiment within the context of efficacy for use within various GIG applications. The protocols chosen for use in the experiment were those that were both freely available from the open-source or not-for-profit development community and were easy to implement in a multi-platform, resource-constrained environment.

The algorithms/packages evaluated included:

a. Optimum Link State Routing Protocol as implemented in the Naval Research Laboratory's NRL OLSR research package.

b. Mobile Mesh Routing Protocol as implemented in Mitre's open-source Mobile Mesh software and the derivative IPMesh (version 2.0) for Microsoft Windows.

c. Ad hoc On-Demand Distance Vector protocol as implemented in LocustWorld's MeshAP bootable CD-ROM software.

2. Compare/Contrast Different Operating Systems and Hardware Platforms for Integration

Several disparate operating systems and hardware platforms were evaluated for suitability as mesh network nodes. Additionally, we attempted to determine to what extent the aforementioned routing protocols were usable across heterogeneous platforms.

a. Microsoft Windows XP Professional

The majority of testing was performed using laptop clients running Microsoft Windows XP Professional Service Pack 1 or later. Additionally, to facilitate some end-to-end analysis and long-haul experimentation, one client in the network operations center (NOC) was a desktop running Windows XP and connected to the network via Cat 5e cable to a central switch. The hardware was a mix of laptops, with the exception of the NOC machine. The laptop makes/models/configurations included:

- Dell Latitude C840, 1.6 GHz Pentium 4, 512 MB RAM, Orinoco Gold 802.11b Wireless PCMCIA NIC
- Dell Latitude C840, 1.8 GHz Pentium 4, 512 MB RAM, Orinoco Gold 802.11b Wireless PCMCIA NIC
- IBM Thinkpad R31, 1.06 GHz Celeron, 256 MB RAM, Netgear MA401 802.11b Wireless PCMCIA NIC
- Dell Inspiron 3800, 746 MHz Pentium III, 256 MB RAM, Lucent WaveLAN Gold 802.11b Wireless PCMCIA NIC

- Dell Latitude X300, 1.20 GHz Pentium M, 648 MB RAM, Lucent WaveLAN Gold 802.11b Wireless PCMCIA NIC

b. Microsoft Windows Server 2003

The NOC also included a client that was formally part of the mesh and was running Microsoft Windows Server 2003.

c. Mepis Linux 2003.10.02

Two of the laptop clients were configured with fully-installed (as opposed to the bootable CD-ROM version) Mepis Linux 2003.10.02. Those laptops were two Panasonic Toughbook CF-73, 1.4 GHz Pentium M, 256 MB RAM, with Orinoco Gold 802.11b Wireless PCMCIA NICs.

d. Windows CE

The four handheld, INTER-4 Tacticomp units were running Windows CE .Net Version 4.20. They have XScale PXA 255 processors with 36KB RAM. They use an 800-miliwatt amplified CISCO 350 wireless chipset, coupled with a 5dBi gain antenna, for 802.11b connectivity.

3. Investigation of Whether 802.11 Mesh is Transportable Over Different Media (802.16/OFDM)

We accepted as a given that properly functioning, local mesh clusters are useful for geometric expansion of the battlespace for small units [(n-1)*d; where n is the number of total cluster members and d is the nominal distance for point-to-point wireless connectivity]. To be useful within the larger context of the GIG and, in particular, in larger-than-squad-sized deployable combat units, a hybrid architecture that incorporates multiple transport protocols and media will most likely be required. For longhaul reachback from a local mesh cluster to a geographically removed tactical operations center (TOC), it is conceivable that various and/or multiple networking technologies will be employed. We attempted to take the OSI Layer 3 mesh paradigm and extend it across an OFDM (802.16 draft technology) backbone to determine whether the latency associated with the mixed PHY and MAC layers would be an issue for the route maintenance that occurs within the mesh.

4. Mesh as an Enabler for Tactical Situational Awareness (SA)

Equipped with mesh-enabled computing devices, the force of the future should be more information–rich than what is currently achievable. Consequently, if implemented correctly and combined with application layer mesh tools, this information richness should give rise to increased situational awareness which, in turn, leads to improved efficiency and operational effectiveness. We attempted to model this improved situational awareness using webcam video streaming, Global Positioning System (GPS) posting, and network node health reporting over the mesh.

5. Ability of NOC to "See" into Mesh Cloud for Management

The final experimental objective was an examination of whether or not the NOC, with its attendant management suite of software, would have full visibility into the mesh. Without the ability to monitor and manage events within the mesh, the usefulness of the NOC to the tactical level wireless mesh network is debatable.

D. STAN 6 EXPERIMENTATION

1. Hypotheses

Our primary hypothesis was that there would be a statistically significant difference in the performance of the routing protocols under consideration based on throughput and network latency time analysis. Our secondary hypothesis was that disparate devices (hardware and operating systems) would behave similarly when running the same, standards-based family of routing protocol. Our tertiary hypothesis was that mobile ad hoc networking could be extended, independent of media, over long (non-line of sight) distances. Our final hypothesis was that network monitoring and situational awareness could be achieved, remotely, through simple network management protocol-based and application level-based tools.

2. Conducting the Experiment

The experimentation consisted of two main methods of testing spread out over four days. The testing was similar between the two methods in that we attempted to stretch the distances between nodes at the same time we were trying to verify multi-hop routing.

a. Side-by-side Comparison Testing

Around the airfield, which served as a physical home to the NOC, we conducted side-by-side tests between MMRP and OLSR to try to determine differences between the two protocols. We used three Windows XP laptops to walk out to distances in which they lost connectivity with the next nearest node. This was to verify our assumptions on geometric expandability of mesh networking between commercial-off-the-shelf, 802.11b-equipped members. Using the Internet Control Message Protocol (ICMP)-based ping and traceroute utilities, we constantly monitored connection binary health (ping as indication of "up" or "down" condition) and route path monitoring (traceroute intermediate nodes). Additionally, the IpMesh program allowed us to view "Reachable IP's" within the mesh. To analyze throughput over the mesh, we used Ixia's Qcheck (Release 3.0) using TCP with a 500kb packet size to be transferred.[37]

Using IpMesh was a straightforward process that just involved launching the program via the Windows GUI, selecting an interface, and then pressing the "Start/Join" button. This activated the two components of the program, the Mobile Mesh Routing Protocol, itself, and the Mobile Mesh Discovery Protocol. This separation of the two components of discovery and routing is what makes MobileMesh unique amongst the mesh protocol implementations.

To enable the NRL OLSR program, we used the command string "nrlolsr –i 192.168.1.X –b 192.168.1.255 32" where X is the specific node that the program is running on, -b enables broadcast to the address that follows, and 32 is masklength of the broadcast address. Although this may have been an improper use of the broadcast address space of the mesh and may have created more overhead, for our limited tests we wanted to ensure route advertisements were being made to the widest possible audience.

b. Pseudo-operational Simulation Testing

Using the most easily deployable of the routing protocols we had at our disposal, NRL OLSR, we attempted to test the behavior of the mesh in a semi-realistic setting. The authors have coined the term "join point" for the node that acts as the

[37] Ixia Corporation, "Qcheck – Network Performance Measurement," <http://www.ixiacom.com/products/performance_applications/pa_display.php?skey=pa_q_check>, Last Accessed 29 Aug 2004.

gateway for mesh traffic transport over other Layer 2 technologies. Similar to an infrastructure-mode access point, this join point forms a central point for reachback. While this makes the mesh more fragile (i.e. – creates a single point of failure) there can be multiple join points if there are multiple communication paths that need to be traversed. We formed a ten-node mesh cluster geospatially oriented as depicted in Figure 9 below. For reference purposes, the semi-static distances between nodes were: 210-217 = 175 feet; 217-213 = 120 feet; 213-218 = 110 feet; and, 210-218 = 405 feet. The mobile nodes, Tacticomps, were 203, 219, 220, and 239. They roamed about to test the self-healing and self-regulating aspects of the urban mesh. The Mobile Join Point Vehicle contained the node (11) that served as a bridge, over the OFDM/802.16 draft longhaul link, back to the NOC. That bridge was a laptop with a MS Windows logical bridge created (and IP address assigned) and NRL OLSR running specifying that logical bridge IP address. The vehicle also contained the OFDM omni directional antenna which facilitated reachback over that longhaul link.

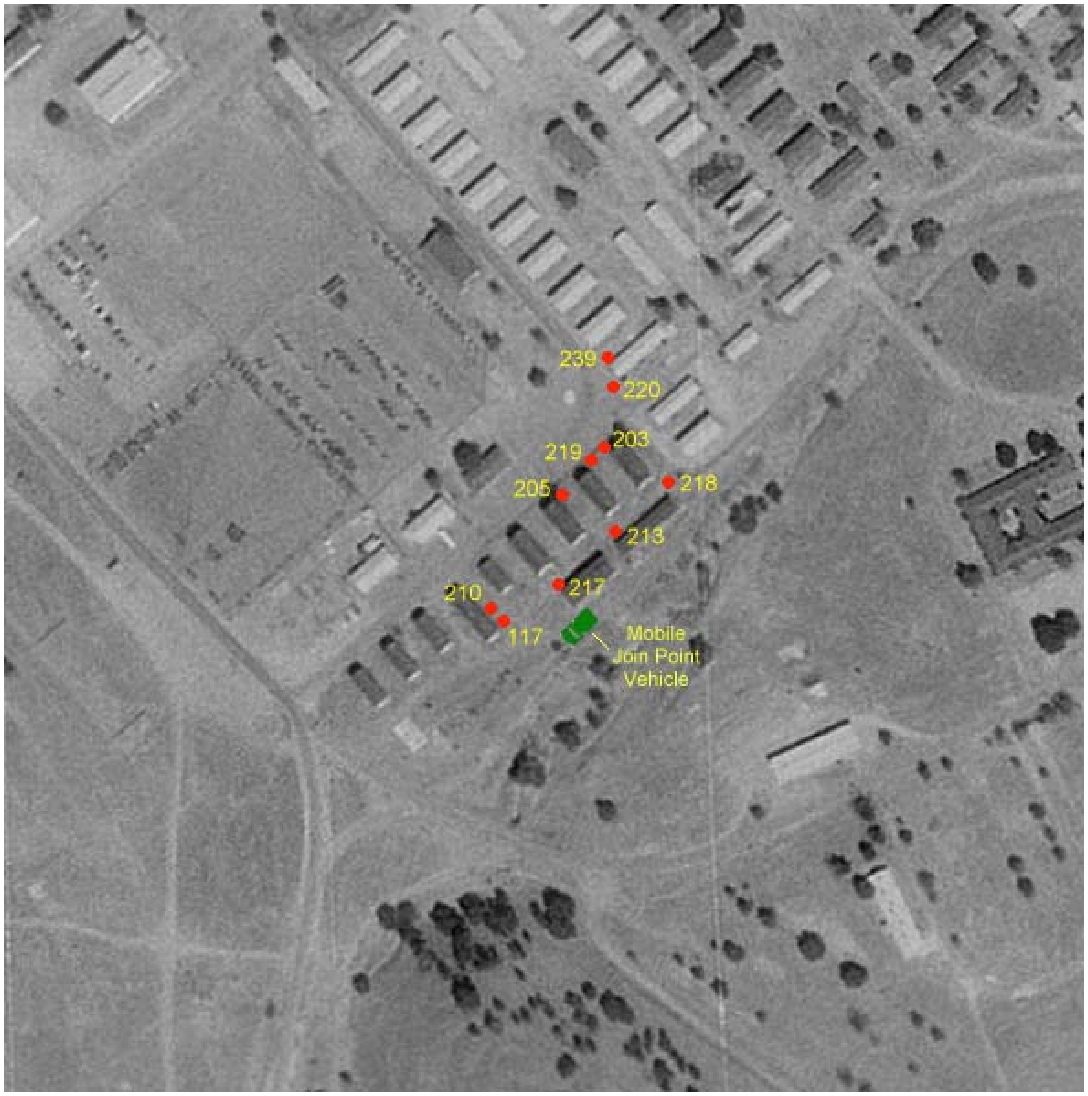


Figure 9. Overhead View of Urban Mesh Deployment

The Mobile Join Point Vehicle made continuous loops around the seven buildings which formed the core of our urban deployment. Data was continuously collected, primarily using ping and traceroute at the node level, to determine connectivity and route paths.

3. Analysis

The results of the tests were analyzed in the context of the two different methods used to test our hypotheses.

a. *Side-by-Side Protocol Analysis*

The side-by-side analysis, based on two-hop routes and a distance between nodes of approximately 180 feet, yielded the data contained in the table below.

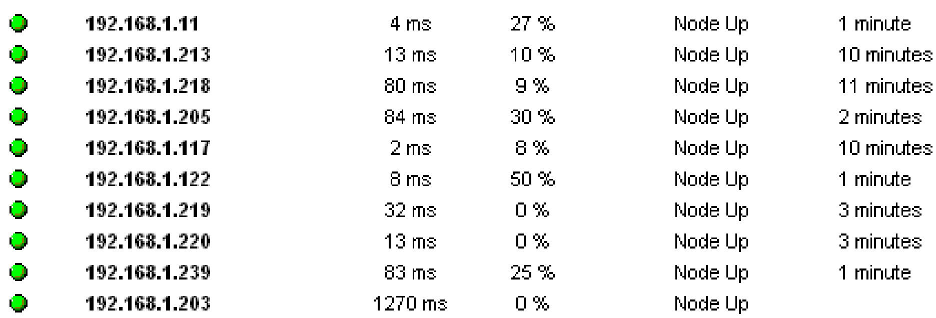
Protocol	Throughput	Ping Time (to root node)	Traceroute Time
MMRP	609.664 Kbps	5 ms	5 ms round trip
OLSR	555.281 Kbps	5 ms	5 ms round trip
AODV	N/A	N/A	N/A

Table 3. Results of Side-by-Side Testing

In addition to the information collected in the strict side-by-side tests, more informal tests of a similar nature were conducted with nearly identical performance characteristics observed. Throughput tests were also conducted before departing the NOC with a single-hop value of 4.5 Mbps (over both protocols) from approximately eight feet from the root node.

b. *Analysis of Mesh Performance in Simulated Urban Operations*

The data from the "urban mesh" was considerably more robust. We were able to observe node health and Simple Network Management Protocol (SNMP) information via the Solarwinds network management software both on-site (at node 210) and remotely (via NOC node 60). A snapshot of node health for the mesh (taken from node 210) is contained in the figure below.



192.168.1.11	4 ms	27 %	Node Up	1 minute
192.168.1.213	13 ms	10 %	Node Up	10 minutes
192.168.1.218	80 ms	9 %	Node Up	11 minutes
192.168.1.205	84 ms	30 %	Node Up	2 minutes
192.168.1.117	2 ms	8 %	Node Up	10 minutes
192.168.1.122	8 ms	50 %	Node Up	1 minute
192.168.1.219	32 ms	0 %	Node Up	3 minutes
192.168.1.220	13 ms	0 %	Node Up	3 minutes
192.168.1.239	83 ms	25 %	Node Up	1 minute
192.168.1.203	1270 ms	0 %	Node Up	

Figure 10. Health of Members of the Urban Mesh

One significant event was a five-hop traceroute that encompassed the following nodes (where the gateway/reachback node (11) performs its function but is invisible to the trace and node 60 represents the NOC monitoring station): 239-220-218-213-217-60. The route table of node 60 (accessed via the "route print" command) is depicted in Figure 11 below. It is clear that true route updates are being promulgated by the NRL OLSR program. Unfortunately, we were not familiar enough with the program to set individual route metric number.

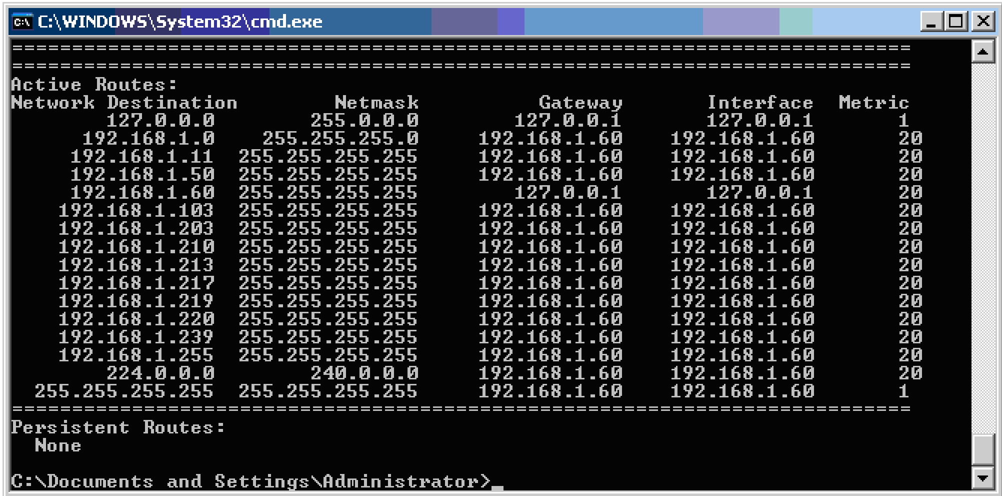


Figure 11. Route Print from NOC Solarwinds Server (as mesh participant)

Situational awareness was maintained over the link through the Situational Awareness Tool developed by Eugene Bourakov at NPS. It allowed remote control of a camera (attached to node 117) before a power failure brought that node down. Additionally, network monitoring tools are contained in the SA Tool that monitor SNMP data and depict throughput and link health.

A detailed depiction of the route table dynamics, observed via Solarwinds from the NOC to node 218, is visible in Figure 12 below. The full route table updates, down to the “next hop” level, are visible via SNMP Object Identifier (OID) 1.3.6.1.2.1.4.21.1.7.

4. Comparison of Results

The results of our side-by-side comparison disproved our primary hypothesis that there would be a significant difference in the performance of OLSR versus MMRP. Though there was a slight dissimilarity in the throughput and ping response times, the fluctuations we observed yielded no clear distinction between the protocols. Using the data from separate side-by-side and the urban environment mesh, we feel we positively proved our second hypothesis that the heterogeneous nodes would behave similarly given a common Layer 3 routing protocol. Through the integration with the OFDM/802.16 draft backhaul from the urban setting, we irrefutably proved our tertiary hypothesis, that

Layer 3 mesh networking is extendable over different lower-layer substrates. We found no instance where a well-formed layer 1/2 infrastructure degraded the performance of the mesh. Our final hypothesis, that effective monitoring and situational awareness could be achieved over the mesh, was proven through the visibility that the NOC maintained out to the edges of the urban mesh.

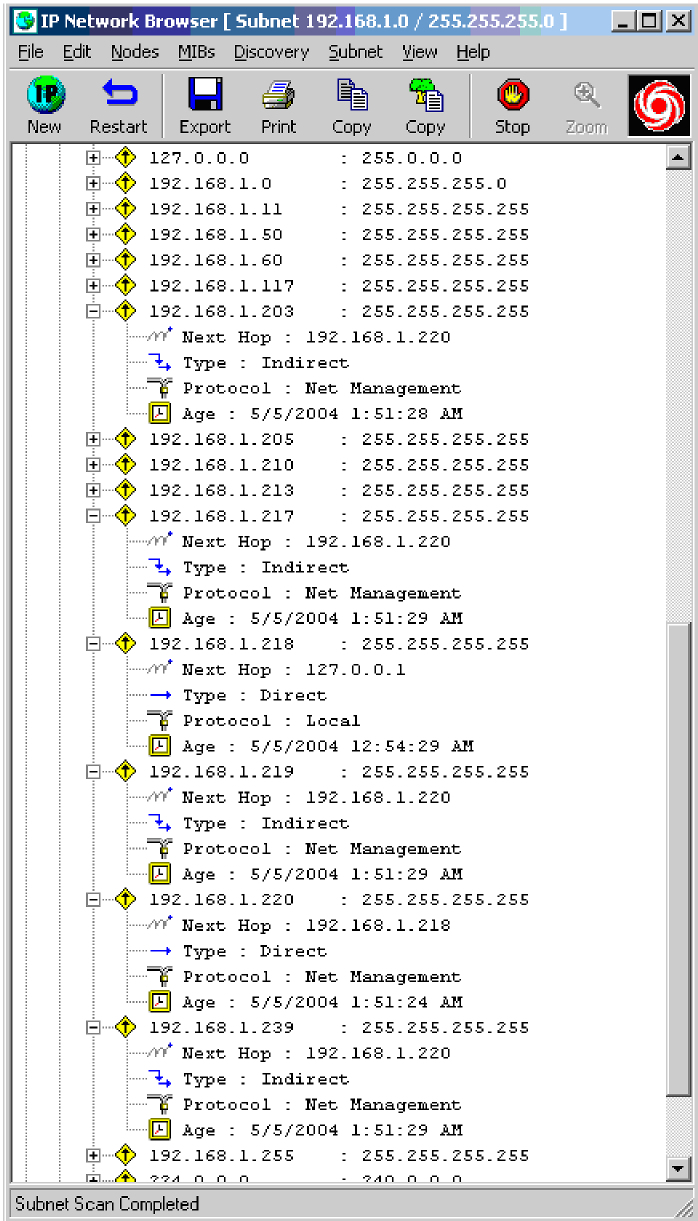


Figure 12. Solarwinds Route Table Entry from Urban Mesh Node as Seen from NOC

5. STAN 6 Conclusions

The choice of OLSR and MMRP, two proactive protocols, was less than ideal as an attempt to get a clear differentiation between available algorithms. Although we saw differences in performance, more testing is warranted to determine the most usable and robust protocol for a highly dynamic mobile mesh. Unfortunately, our attempts to modify the LocustWorld AODV implementation for local use produced no usable data. There are a wide-range of choices starting to emerge for layer 3 protocols that need to be systematically examined in order to determine feasibility for rapid reconfiguration environments like the STAN network. Once mature, wireless mesh networking will become the “killer enabler” of the GIG for the force of the future. Hybrid architectures that leverage aggregating “join points” for deployment of multi-level meshes will create an interlaced wireless battlefield with the ability to move larger amounts of data much more quickly than is currently possible. The robust nature of the mesh segments with their ability to self-form, self-heal and rapidly adjust to changes in their operating environment make them the mode best suited for small-unit operations where mobility and situational awareness is paramount. The ability of the mesh to rapidly expand outward geometrically, with range between nodes independent of one another, is one of its greatest assets within the context of the mobile warfighter.

E. NPS TESTBED EXPERIMENTS

We performed several discrete experiments on campus to continue our investigation of mesh behavioral characteristics, protocol comparisons, and usability. These experiments were usually approached with limited objectives in mind. For our outdoor testing, the goal was primarily to examine the effective ranges of our laptop nodes. The specific protocol behavior was a lesser focus. Our indoor tests centered on trying to obtain a true differentiation in network characteristics and metrics between the different protocols we had to work with.

1. Extendability and Usage Testing (Indoor/Outdoor)

Over the course of our research, we conducted several campus-based experiments that took place from the Global Information Grid Applications (GIGA) lab and extended outward in multiple directions. Our testbed consisted of the following laptops:

- IBM Thinkpad R31, 1.06 GHz Celeron, 256 MB RAM, Netgear MA401 802.11b Wireless PCMCIA NIC (192.168.1.1)
- Dell Latitude X300, 1.20 GHz Pentium M, 648 MB RAM, Lucent WaveLAN Gold 802.11b Wireless PCMCIA NIC (192.168.1.2)
- Dell Inspiron 3800, 746 MHz Pentium III, 256 MB RAM, Lucent WaveLAN Gold 802.11b Wireless PCMCIA NIC (192.168.1.3)
- Panasonic Toughbook CF-73, 1.4 GHz Pentium M, 512 MB RAM, Lucent Orinoco Gold 802.11b Wireless PCMCIA NIC (192.168.1.5)
- Panasonic Toughbook CF-73, 1.4 GHz Pentium M, 512 MB RAM, Lucent Orinoco Gold 802.11b Wireless PCMCIA NIC (192.168.1.6)

a. Accordion-like Spreading

Simply arraying a series of nodes across the campus, we were able to verify that our generalized expansion theory was possible over a small number of hops. Our simple expandability expression is (n-1)*d, where n is the number of nodes in the mesh and d is their nominal, effective radio range.

As seen in the figure below, a graphical depiction of a representative experiment conducted on April 27, 2004 at NPS, the geometric expandability manifested itself nearly exactly as we had predicted. We conducted the experiment for about ninety minutes, beginning at noon, on a clear day with the temperature around sixty-five degrees Fahrenheit.

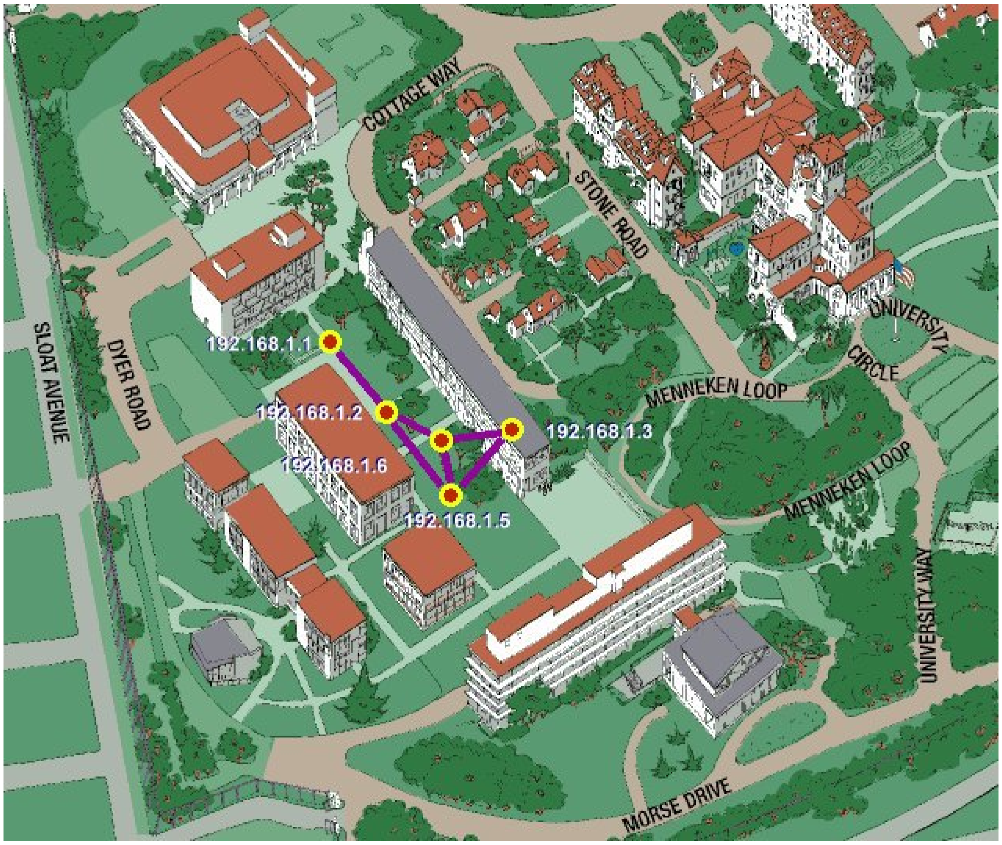


Figure 13. Accordion-like Spreading Example

The nominal distance between each of the nodes 192.168.1.1, .2 and .5 was approximately seventy-five meters with several large trees interspersed. Solid links were established and maintained at those distances with Internet Control Message Protocol (ICMP) packets (ping and traceroute) used to verify link state.

b. Metrics

We monitored the routing topology, link health and status, and bandwidth information in each of the nodes, with special focus on the logically farthest pair.

The route taken for the end-to-end, three hop bandwidth measurement is displayed in Figure 14 below. Significantly, although 192.168.1.6 was physically closer to .2 than .5, the best logical route was through .5. This may have been because of the route load on .6 at the time of the test or radio strength between the communicating nodes.

```
Tracing route to 192.168.1.3 over a maximum of 30 hops

  1     *        3 ms     4 ms  192.168.1.2
  2     7 ms     7 ms    14 ms  192.168.1.5
  3    15 ms    14 ms    17 ms  192.168.1.3
```

Figure 14. Traceroute from 192.168.1.1 to 192.168.1.3

The bandwidth recorded over that three-hop segment, using the MobileMesh Routing Protocol, is displayed in the following figure. We observed significant bandwidth degradation per hop, but the raw bandwidth is still rather high, given the three hop path at a fairly long radio distance between nodes.

Figure 15. Qcheck TCP Throughput Calculation

c. Usability Observations

During all of our campus-based experimentation, we experienced some inconsistent link health when loaded down with application-level usage tasks. Our iterative, layer-oriented approach to testing helped us determine the general usability of current mesh solutions, however.

We purposefully began with Internet Control Message Protocol (ICMP) ping and traceroute utilities that are fairly small in size, seventy-four and one hundred six bytes, respectively. After we achieved stability and recorded our baseline throughput measurements, we attempted to use video conferencing with Microsoft's NetMeeting over the three-hop route. The results of the streaming video test proved more problematic than the raw bandwidth number would have led us to anticipate. Jitter, ghosting and stream interruption were all encountered during our NetMeeting call. Whiteboarding and text-based chat functions were nearly real time, but unicast video was certainly not optimized for route topology changes.

2. Real-world Comparison of OLSR and AODV (Indoor)

The testbed for our targeted comparison of OLSR and AODV was the same heterogeneous pool of laptops utilized in the outdoor, general protocol behavior study. During this round of experiments, however, we chose the second floor of the Dudley Knox Library at the Naval Postgraduate School as our test environment. This allowed us the flexibility to place our nodes at sufficient distances to demonstrate mesh behavior while keeping them close enough for monitoring and reconfiguring tasks. The library's books also served a useful role as energy absorbent material to give us a realistic representation of indoor 802.11b ranges.

A top-down view of the node placement with approximate distances is contained in Figure 16.

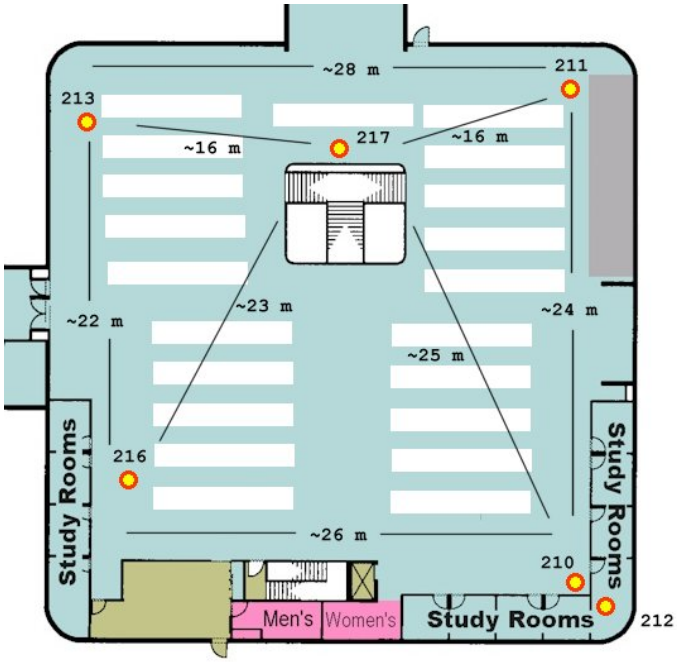


Figure 16. Indoor Mesh Experiment

The star-shaped layout was chosen to maximize the probability of alternate routes being taken if tenuous links emerged somewhere within the network. We compared the NRL OLSR variant with the Intel-developed AODV program for connectivity, general behavior, latency and bandwidth. Additionally, using the Solarwinds management suite, we maintained a constant picture of packet loss and general traffic on the medium. The final experiment was conducted on July 30, 2004, over the course of two hours with laptops plugged in and running exactly the same programs with the exception of the protocol stack. All other conditions were as identical as possible.

a. Behavioral Generalizations

Overall, the protocols behaved as we expected they would, given the operating environment and non-mobile nature of the mesh. The AODV program contained a provision to monitor the routing table from inside the program. It provided near real time updates that allowed for easy monitoring of network route topology changes. As expected, the AODV tables were relatively empty until there was data to be routed through the network.

In contrast, OLSR route table updates were much more populated and static over the course of the test. Unfortunately, we were not able to capture any real time data and resorted to frequent "route print" commands at the command line for table monitoring.

b. Latency and Bandwidth

One of our primary goals with respect to testing the two different protocols was to attempt to draw conclusions about the differentials observed in both network latency and bandwidth availability. We again employed the Qcheck software tool for evaluation of response time and throughput between logically "farthest" nodes pairs. Two main differences emerged as we performed identical operations on the same nodes.

First, with respect to latency, the ICMP traceroute packets showed an interesting, recurring difference in the latency of at least one of the hops. Figure 17 below is a side-by-side representation of the latency phenomenon. OLSR is depicted in the left block while AODV is on the right over the three-hop route connecting 213 to 212.

Figure 17. Latency Difference Example – OLSR vs. AODV

We surmised that the increase in latency on at least one of the links was the result of the reactive nature of the AODV protocol. By having to actively "rediscover" the link when traffic needed to flow over it, the latency to build in the route likely caused the spike in response time. OLSR, on the other hand, attempted to keep itself updated at all times and the link latency numbers all fell roughly in line with one another.

Bandwidth also exhibited tangible differences between the two protocols. As evidenced by Figure 18 below, conducted over the same three-hop path from 213 to 212, there was a marked improvement in throughput when using the AODV implementation. It is important to note, however, that the throughput test was conducted immediately following a traceroute operation in order to verify the path from source to destination. As a result, the route paths were built into AODV before the bandwidth test was conducted. We ran one test where we assumed connectivity and route paths, and the throughput levels were nearly identical to the OLSR numbers. The overhead associated with the route setup operations was directly in line with the constant route maintenance functions in the proactive protocol.

Figure 18. Throughput Difference Example – OLSR vs. AODV

Overall the differences were discernible but not significant enough to draw a "best of breed" conclusion. In a static or low mobility environment, the routing overhead generated with on-demand route discovery functions is outweighed by the throughput gain owing chiefly to packet delivery ratio improvement over proactive mechanisms.

3. Application Layer Tests

Using the same heterogeneous mix of testbed nodes, we attempted to predict and realistically test the behavior of certain applications riding atop the lower-layer mesh substrate. Without the assistance of a common framework for data interchange, we were skeptical of the usability of some common communications applications.

a. Groove Networks' Virtual Office

Groove Networks' Virtual Office Version 3.0 is a commercially available collaboration application that operates on several physical and logical interconnection levels to maximize synchronization and situational awareness of the end users. Users work together in "workspaces" that are a collection of shared productivity tools that allow common contextual communication and information sharing. Familiar collaboration tasks such as one-to-one and one-to-many text and voice messaging, file sharing, project management, calendaring, and whiteboarding are all included.[38]

By using a multi-faceted, distributed connection framework, Groove allows peer-to-peer interaction and synchronization as well as synchronization through a relay server that operates on a store-and-forward basis. Because Groove is engineered and optimized for peer-based ad hoc interaction, we were anxious to test its performance over a multi-hop construct.

We loaded the Virtual Office application on each of the mesh nodes in our testbed and set up a shared workspace that served as the central area for multicast data exchange. Workspace setup and connection verification was accomplished while the wireless nodes were all within 802.11b ad hoc range of one another. We then proceeded to move our nodes into a ladder-like, multi-hop configuration. A minimum of two hops was our desired goal between logically farthest links in order to conduct operational tests throughout the mesh.

The application, which provides a visual representation of all nodes within the workspace, dropped nodes as the links were lost and reacquired them as the links were restored. Additionally, there was no instance of the multi-hop environment causing Groove to become confused in rendering member participation status.

The most obvious issue we encountered was loss of connectivity because of the overhead associated with the application itself. All Groove communications are encrypted by default. That fact, coupled with the frequent topological updates the program performed, created a significant burden for the mesh implementations we used. Even more specifically, multicast messages that went to every user within the workspace, including the common text chat, whiteboard and picture gallery tools, caused much more slowdown and link stress than the unicast “messages” that can be exchanged between users.

In summary, while we were pleasantly surprised at how well the ad hoc features of Groove handled the underlying mesh routing and topology changes, we were

[38] Groove Virtual Office, Product Backgrounder, July 2004, <http://www.groove.net/pdf/backgrounder/GVO-backgrounder.pdf>, Last Accessed 08 Sep 04, 14.

slightly disappointed by the "weight" of certain features of the application on the already fragile mesh. Multicast, a realistic requirement for any military application, must be optimized by Groove or a third-party instrument for use over the mesh substrate before effective application-level communication and collaboration is realized.

b. Browser-based Testing

Running Microsoft's Internet Information Server (IIS) on a single node within the mesh allowed us to test and evaluate information exchange from the point of view of a near-ubiquitous, open-standard networking technology. Additionally, using our "join point" reachback path to the wired network inside our NOC during the STAN experiments, we were also able to utilize web browsers for common information retrieval tasks.

The Hypertext Transfer Protocol (HTTP) seemed to have no issues with the mesh as provided at the lower layers. While data throughput was slowed by the join point and multi-hop paths, web browsing was relatively unaffected by our mesh architecture. It is important to note, however, that most of the browsing we did was nearly stateless and that more complex, stateful interactions would likely encounter problems with a constantly changing lower-layer path.

F. COMPOSITE FINDINGS AND COMMON THEMES

With the broad-based goal of all the experiments and trials to be the realization of the methods to achieve the hybrid mesh integration and fusion discussed in Chapter III, we distilled some common themes and findings that work toward that objective. While no end-to-end panacea was discovered, we were able to gain a much better understanding of the complexity of the problem space, moving forward.

1. Results of Protocol Comparisons

The overall aggregated results for our Layer 3 protocol comparisons were generally in line with the published literature on performance patterns. The simulation results we examined were useful for benchmarking purposes, only. Nearly all of the modeling and simulations were overly optimistic with regard to throughput and scalability. This may be partially due to the fact that most network simulation programs fail to take into account the processing overhead associated with today's commonly used operating systems and treat the issue of network routing from a more focused, "pure" perspective.

AODV seemed to provide slightly more usable paths once the unicast routes were discovered, but the latency in setting up the routes was discernible. OLSR definitely provided quicker access for unicast interactions, but the overhead that was constantly on the medium was detectable. Our use of MMRP in the outdoor experiments followed, roughly, the behavior noticed in OLSR.

Node mobility in each of the experiments was random and low-speed, so a judgment on which protocol family handles mobility better was not possible. However, we can reasonably assume that OLSR handles mobility a bit better than AODV by virtue of OLSR trying to maintain an accurate picture of the topology and not depending on late discovery which may drive complexity and overhead message count much higher.

2. Agent-based Services Behavior

Agent-based services seemed to be ideally suited for operation over the mesh. Two examples stand out in our testing. The SNMP agents used by the Solarwinds suite caused very low overhead on the network and were consistently available to report SNMP data. The agent-based Situational Awareness application was also very stable with respect to the agent polling and reporting that occurred over the mesh.

Because of their typically small footprint on the network landscape, agent-based services and applications have a vital role to play within military mesh networking. The value proposition of agent-based mechanisms versus the cost in data "weight" makes them very well-suited to assuming an even more prevalent role within the bandwidth limited mesh networking environment.

3. Application Layer Potential

Based on our results with Groove and web browser applications, with some modifications the application layer seems well-suited to accommodating mesh behavior and assisting with mesh management functions. If there were a common services layer-like application product line located somewhere between Layer 3 and the application layer, as we have outlined with the Mesh Routing Capabilities Toolset, applications could be even more efficient and adept at working over the mesh.

V. TOWARD APPLICATION LAYER MESH

A. INTRINSIC CHARACTERISTICS OF UPPER LAYER MESH

1. Leveraging the Underlying Substrate

To consistently use the information passed at the lower OSI layers, there are certain assumptions that need to be made regarding the reliability of those layers. As protocol development continues to evolve, the ubiquity of the physical network will become more constant in everyday life and battlefield operations. When the underlying substrate achieves a six-sigma (99.9999%) or greater availability metric, the application layer will necessarily begin to emerge as the focal point for the next generation of communications enabling technologies. This lofty goal, however, may never come to fruition in a constantly shifting wireless mesh network. There may be techniques, however, that can better leverage the improving physical, link and network layers to bridge the gap and move toward the desired states of nearly perfect availability.

Radio frequency (RF) spectrum usage and multiple-access method advancements continue to emerge that will commoditize the novelty of persistent and pervasive, high bandwidth connectivity. Whereas wireline networks still bear the weight of most of the global network load, tomorrow's networks will leverage much more of the available airwaves. While the 802.11b specification supports data rates of up to 11Mbps, there are now related, proprietary products that claim to support ten times that number of bits per second. How best to couple the physical and link layer scheme advancements with usability will, eventually, fall to the upper OSI layers.

2. Pseudo-Algorithms

Certain operating parameters and heuristics exist, when considering Layer 3 mesh routing protocols, which are common across the families of protocols. The generic mechanism to find relay information paths from point-to-point through an intermediary (route discovery), the constant issue of which path to choose for information exchange (route optimization), and characteristics of peering nodes (nodal awareness) are all important for routing and data exchange throughout the network. Examined not just as heuristics, but as pseudo-algorithmic constants, these three items become the building blocks for a better method to communicate meaningful data across a network.

a. Route Discovery

Communication paths to other nodes form the concrete manifestation of network topologies. Whether considering a packet or circuit-switched network, the path from one node to one or many other nodes must be established before messages can be passed. End-to-end addressing methods, as outlined in Chapter III, greatly simplify the task of moving data for transient, loosely coupled or mobile peers.

b. Route Optimization

Apart from finding "a" route through a network, finding the "best" route is often an insurmountable challenge with mobility and heterogeneity factored in. Different metrics are used to define "best" within the routing universe. Intricate trade-offs must somehow be done to ensure the paths chosen are, indeed, the best for the particular topology, degree of volatility, and nature of the data being communicated over the network.

c. Nodal Awareness

One of the more important, yet slightly abstract, operations that occur in network routing is the idea of nodal awareness, or the discovery and utilization of the capabilities of other nodes on the network. This concept of capabilities, both concrete and logical, may be the linchpin for future advancements on the standard routing paradigm.

B. THE MESH ROUTING AND CAPABILITIES TOOLSET

Given the ever-improving connectivity picture and the naturally occurring methods of data exchange and routing, wireless mesh networking may be the key enabler to realizing the promise of ubiquitous connectivity. Few information technology solutions are as obvious as that of mesh being the key to pervasive computing environments. By making every node a routing, vital piece of the infrastructure, the potential exists for a robust, woven network fabric that spans the continuum of the GIG. Multi-hop routing not only extends the reach of the network, but also allows the inherent redundancy it brings to be leveraged for other purposes. If there were some way to optimize the possible reliability and availability gains, two of the most promising quality attributes of mesh routed topologies, then the capabilities of the most remote nodes could be leveraged for a variety of different purposes. The flow of intelligent information, improved situational awareness, and the overall value of every node on the network would drastically increase.

In order to realize the potential of the lower layer wireless mesh, however, an application layer, or near-application layer, product line needs to be put into place to broker the required services and data exchange tasks. We believe the Mesh Routing and Capabilities Toolset (MERCAT) will fill the void that currently limits the benefits that should be reaped from the emerging wireless mesh maturity. We propose a product-line architecture approach for a family of semi-generic software components and products that will be open-architected for maximum flexibility in design and implementation. Product-line architecture is defined as, "the common architecture for a set of related products or systems developed by an organization."[39]

1. Domain Description

Near-application layer mesh networks, as implemented through the components and services of the Mesh Routing and Capabilities Toolset, will be responsible for optimizing quality of service and application behavior based on basic routing information gathered from the topology of the network. Additionally, through the use of intelligent agents operating with ontological awareness of their operating environment, capabilities of other nodes will be leveraged according to changing environmental influences and end-user desires.

There is a wide range of computing assets that will need to be leveraged within the GIG construct. Unattended Ground Sensors (UGS), man-portable devices, embedded vehicular systems, and tactical (and higher echelon) operations centers are all part of the distributed computing continuum. Between the endpoints of the continuum, there are two interrelated sub-domains that hold the key to usability for pervasive computing constructs. The first sub-domain is an underlying logical process that connects an end-node sensor back to the mechanism that seeks to employ it. The second sub-domain is

[39] Jan Bosch, *Design and Use of Software Architectures*, (London: Pearson Education, 2000), 162.

the communications sub-domain that makes possible the flow of relevant data across the physical implementation of the network.

a. Logical Sub-domain

Within the logical framework of the generalized "sensor-to-shooter" chain, there are certain dependencies, conditions, expectations and elements that can be conceptualized and enumerated. Logically, working from source to destination, down a decision tree from a potential range of courses of action for an operator node, a set of probabilities exists that some terminal condition will be met at the sensor node. Within the decision tree, there may be an extensive range of factors that drive the probability of "success" either up or down. Success has two elements and is defined as a specific terminal condition being met *and* being made known to the operator. These factors are directly related to the behavior or the communication sub-domain.

Derived from the logical sub-domain is the concept of the resultant decision matrix. That is, courses of action are more or less desirable and will tend to be taken if there is a greater likelihood of the enabling terminal conditions being met, subject to the probability of them being reliably communicated. Differential influences may include (but are not limited to) conditions such as lack of all relevant data, lack of data currency, lack of verifiable data veracity, unreliable sensor behavior, and an incomplete or ill-defined decision matrix. Once again, the impact of the communications sub-domain becomes highly relevant once the logic is clear.

b. Communication Sub-domain

The implementation of the logic is relegated to the communication framework which, moving from higher to lower levels of abstraction, is the network that forms the GIG. The functionality of the communications sub-domain has a recursive impact on the probabilities of success contained within the logical sub-domain. Without the network, there is no logical link from sensor-to-shooter.

A graphical depiction of the interrelationship of the two sub-domains within the larger context is presented in Figure 19.

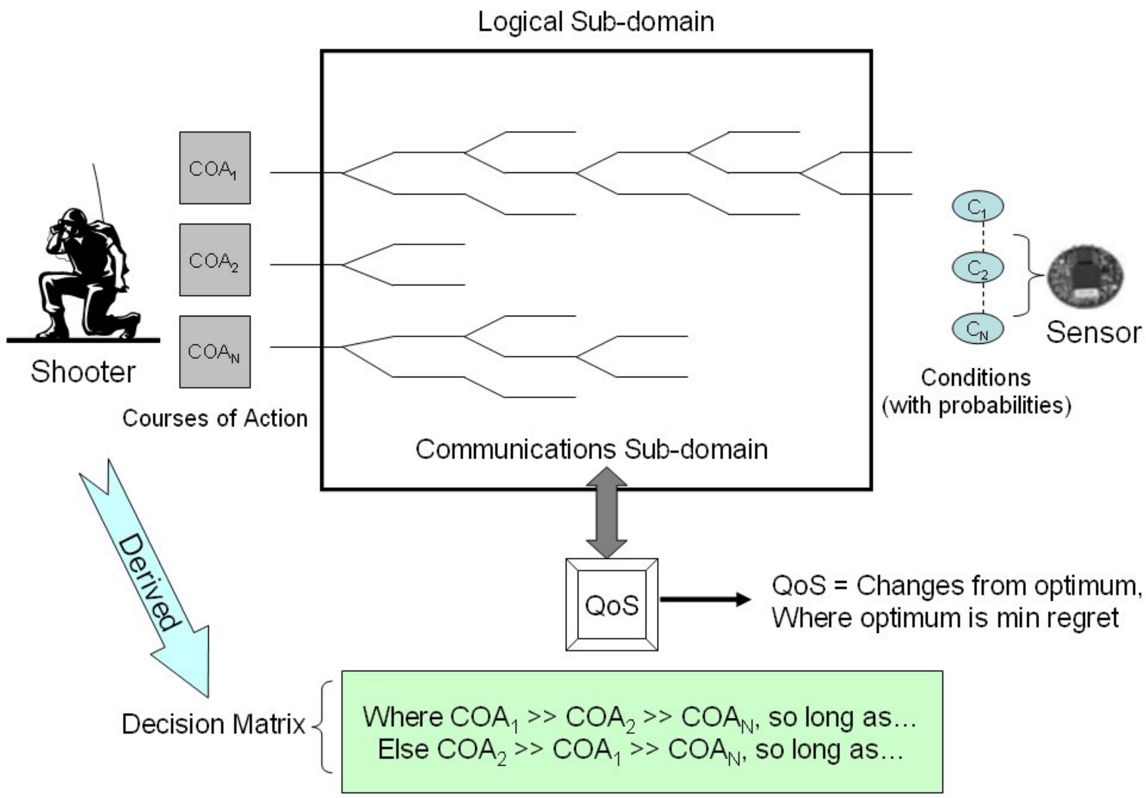


Figure 19. Netted Sensor-to-Shooter Domain Description

The vital piece that links the two domains is the concept of quality of service (QoS). Change from the optimum, that is the minimum regret equation that seeks to minimize the probability of losing some value times that expected value, is the best way to describe the theory of true quality of service. Although much has been written and postulated about an absolute quality of service metric, we believe the only way to achieve a workable QoS is by integrating some intelligent reasoning into that component and building a dynamic, ontologically-aware quality of service. This element is central to the MERCAT product line and, if implemented correctly, will enable the flow of information from the external warfighting environment, through a higher-functioning communications framework, and ultimately shape the plans and courses of action in order to achieve and maintain a dominant information position.

2. Functionality Demonstrated Through a High-Level Use Case

Remote capability discovery and invocation are two aspects of MERCAT that will drastically improve the functionality of nodes operating throughout the distributed mesh structure. The following "brief format"[40] use case illustrates, in generic terms, how a MERCAT-enabled warfighter of the future might operate within the higher layer mesh networked environment:

Leverage Sensor

Main Success Scenario: A ground-based, fully-networked warfighter advances over contested terrain that has been seeded from the air with wireless mesh networked sensors. He is part of a heterogeneous wireless mesh network that has self-formed as soon as the nodes were powered up. He receives an alert on his wireless mesh augmented reality unit that several tripwire sensors have been activated about two kilometers from his present position. His system immediately alerts him to the presence of a covert, high-definition, pan-tilt-zoom camera/laser designator that is collocated with the tripwire sensors that have been activated. He is able to select that specific camera on his heads-up-display unit, slew it and view the video of a squad-sized enemy unit headed towards him. The intelligent agents within the network have maximized the quality of service metrics for the data in and around the area of interest so the video he receives is near-real time, even over the multiple-hops of the mesh. He calls in fire support on the exact location of the enemy and illuminates the target as the laser-guided projectile is precisely delivered. Although the tripwire sensors in the immediate vicinity of the targets have been rendered inoperable, the wireless mesh self-heals and the quality of service agents adjust to optimize the bandwidth so he is able to conduct a battle damage assessment sweep with the mesh camera.

There are many elements that have been omitted for brevity and clarity, but the utility of a MERCAT-enabled battlespace is clear. By facilitating best route path choices, optimizing those paths, and providing the opportunity to leverage capabilities of the end nodes, the collection of components that make up MERCAT will become a transformational stepping stone to the realization of end-to-end utility within the GIG. These components, however, must be well-designed and maintain their open systems identity to maximize the quality attributes of our proposed solution.

[40] Craig Larman, *Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and the Unified Process*, (Upper Saddle River, NJ: Prentice Hall PTR, 2002), 46.

3. Quality Requirements

While MERCAT is intended to enable and help provide the functionality described in the use case above, the system needs to be designed to support various software quality requirements, as well. Several of the most important quality requirements are delineated below.

a. Performance and Near Real Time Behavior

The performance of MERCAT will be dependent on many other network nodes and the interfaces into the system. Components need to be designed that optimize performance within the context of their physical implementations. Because we envision MERCAT being deployed on a wide range of computing devices, the software must remain open and light enough to accommodate being pushed to limited power devices. A related quality attribute is the near real time behavior that will be required to make the distributed communications links viable.

b. Reliability

Reliability will be integral to the components that comprise MERCAT. Efficient, yet lightweight, error-handling methods must be built into the software to avoid loss of data or disruption of the information flow across the network.

c. Maintainability and Configurability

The components of MERCAT must be designed for the easiest maintainability levels possible. New hardware will be rapidly integrated into the GIG and the software needs to be maintainable across the spectrum of new equipment. A standard process for recognizing new interfaces, yet maintaining core functionality and interoperability will be essential.

All the components within MERCAT must be easily configurable in the face of changing hardware, routing mechanism breakthroughs, and the expansion of capability sets on the end nodes. By using common data interchange mechanisms, like XML, configurability of the open-architected components should be straightforward.

4. System Context and Interfaces

The main interface into the MERCAT system will include the planning and collaboration elements that form the higher-level decision support systems of the GIG.

The physical network routing data and the capability data contained within the nodes, themselves, are both extremely important interfaces. While the end-state goal is to have MERCAT touch every part of the GIG and make the concept of external interfaces something of an misnomer, the reality during the transition will likely be that a majority of applications already present within the GIG will need to interact with the core functionality of the toolset in order to begin the long journey to full capability sharing. A generalized depiction of the interfaces between the system, the decision making apparatus and the physical entities is included in Figure 20 below.

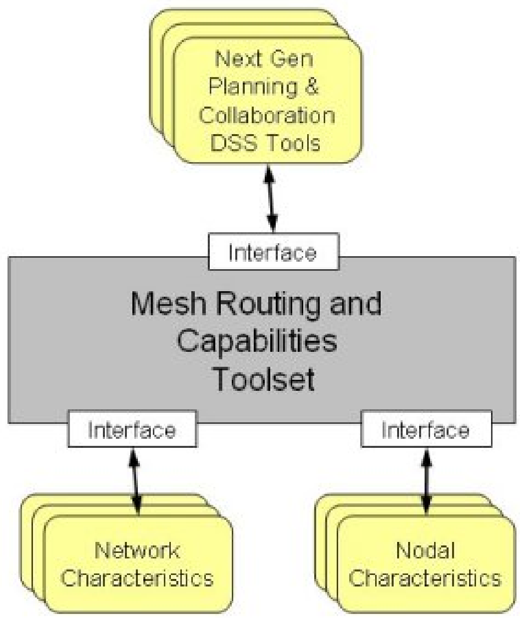


Figure 20. Interfaces of the MERCAT Framework

5. Main Components and System Instantiation

The main components that make up MERCAT are illustrated in Figure 21 below. Although represented as objects with high-level attributes and methods, we are simply using this abstraction to try to clarify and demonstrate the theoretical composition of the product line, not specify the design process, itself. Any number of different development methodologies could produce an appropriate set of components to meet the functionality and quality requirements described here.

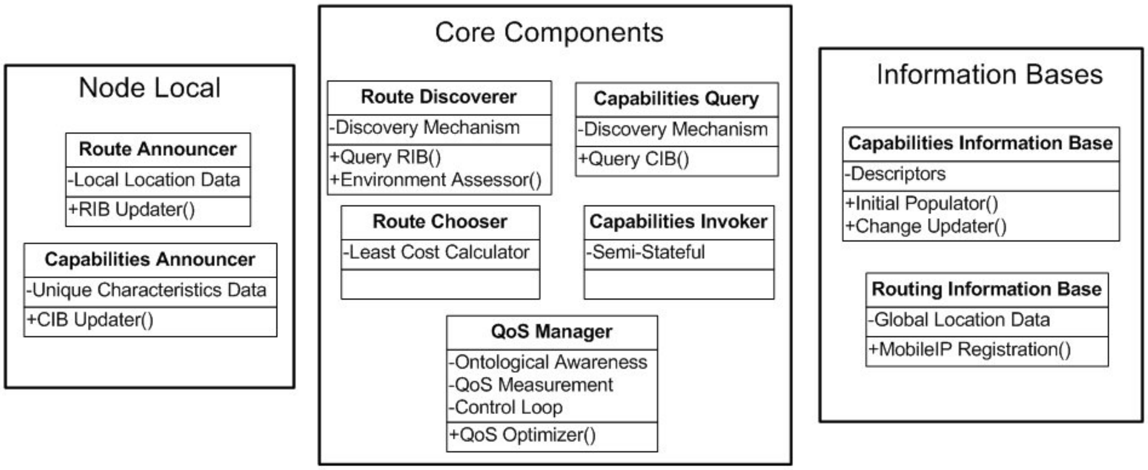


Figure 21. Component Architecture for MERCAT

The general interaction between the generic components forms the basis of a MERCAT instantiation. A description of that interaction is helpful to understand the mechanics of the system.

The “node local” set of components is distributed out to each of the mesh nodes. The routing and capabilities announcement mechanism can be implemented either through a push or pull service. The other distributed set of components is the two “information bases.” While we fully expect every node to have completely updated capability and location addressing data contained within it, a remote replication of the known capabilities and a location vectoring scheme for mobile addressing are envisioned as high-level, replicable data repositories.

The core components of MERCAT are the route discovery, route choice, capabilities query and capabilities invocation pieces. These four components do the bulk of the work when trying to determine where a node is and how it may be leveraged. These components have direct interfaces both up the distributed tree to the information bases as well down the tree to the nodes themselves. Courses of action are married to terminal conditions through the data that is exchanged by these components.

The final component is the QoS manager. Although this is technically part of the core component group, it is this element that makes MERCAT a powerful, unique conceptual system of systems. The QoS manager will include a level of ontological awareness that is absent from present day QoS tools. By being privy to the important data elements and the reasoning behind course of action prioritization, this smart QoS will be better able to optimize the state of the network through a robust control loop that measures the health of the mesh and interacts with the routing and capabilities components to identify the best paths for the best nodes. The free flow of communication between all the distributed segments over the ever-improving mesh will usher in a dramatically transformed way to fight and win future wars fought for information superiority.

C. MESH NETWORKING MARKUP LANGUAGE – THE DATA INTERCHANGE VOCABULARY

For the MERCAT framework to facilitate seamless data exchange and parsing, it must have a common linguistic framework at its core. We envision a new, high-level XML vocabulary for handling the Web services-like messages that individual nodes will exchange. Our proposed MeshNetML schema provides a specification for the structured interchange of information between and among nodes within the MERCAT-enabled mesh.

1. MeshNetML Overview

The MERCAT architectural framework in which we envision MeshNetML residing is likely to encompass many different data interchange mechanisms. This services-based, product-line architecture is ideally suited for the types of data we anticipate passing and the handlers that will act upon that data. In order for the components that comprise MERCAT to be efficient, we believe the best answer is an extensible set of essential data elements that will be very similar to SensorML's schema contents, yet at a much higher level of abstraction. We envision something akin to the SNMP's streamlined, tree-based Object Identifier mechanism to handle the capability characteristics of the nodal data.

a. Essential Data Elements

While the universe of descriptors for computing nodes is immense, there are a core set of data that can describe the essential identifiers of both routing and capabilities within a network entity. We have chosen to include the node's identification data using the IPv6 subnet router addressing model complex type, a general categorical grouping choice compositor complex type, as well as the capabilities complex type with one-to-many occurrences.

b. Extensibility

Just as IPv6 employs the concept of extension headers to accommodate non-standard delivery and forwarding options, MeshNetML should have data containers that can flex to include non-recurring information of interest. The use of extension header-like fields to describe the capabilities within a node will enable most MeshNetML datagrams to be very small and efficient. However, if more data is required, the flexibility is built in to accommodate growth and higher-order operations.

c. Proposed Basic Schema

An example of a basic, node-description schema that incorporates some of the essential data elements is presented in Figure 22. This simple schema includes the IPv6 addressing information, the general category of the node, and the capabilities resident within the node. This represents the descriptive data within the node itself, so it can be leveraged for use in the MERCAT structure. Obviously, much more data about a node needs to be promulgated for it to be useful to the mesh at large, but this schema represents a starting point for further research and exploration into how to accomplish the data interchange between nodes using an XML vocabulary.

D. DEVELOPMENTAL ROADMAP

The framework for MERCAT and MeshNetML is still being developed and, as such, more work needs to be done to flush out the semantic and syntactic elements and relationships that will make the high-level architecture and its core vocabulary a reality. In addition to the complex tasks of completing the architecture, more fully expanding the internal data definitions, and building and validating the XML schema, a transition roadmap needs to be outlined that will describe the path forward in order to realize our implementation goals.

We foresee initial implementation through a standalone, MERCAT-layer or passthrough “filterlet.” This add-on construct will allow current applications to function normally while proving the viability and soundness of the application layer MERCAT

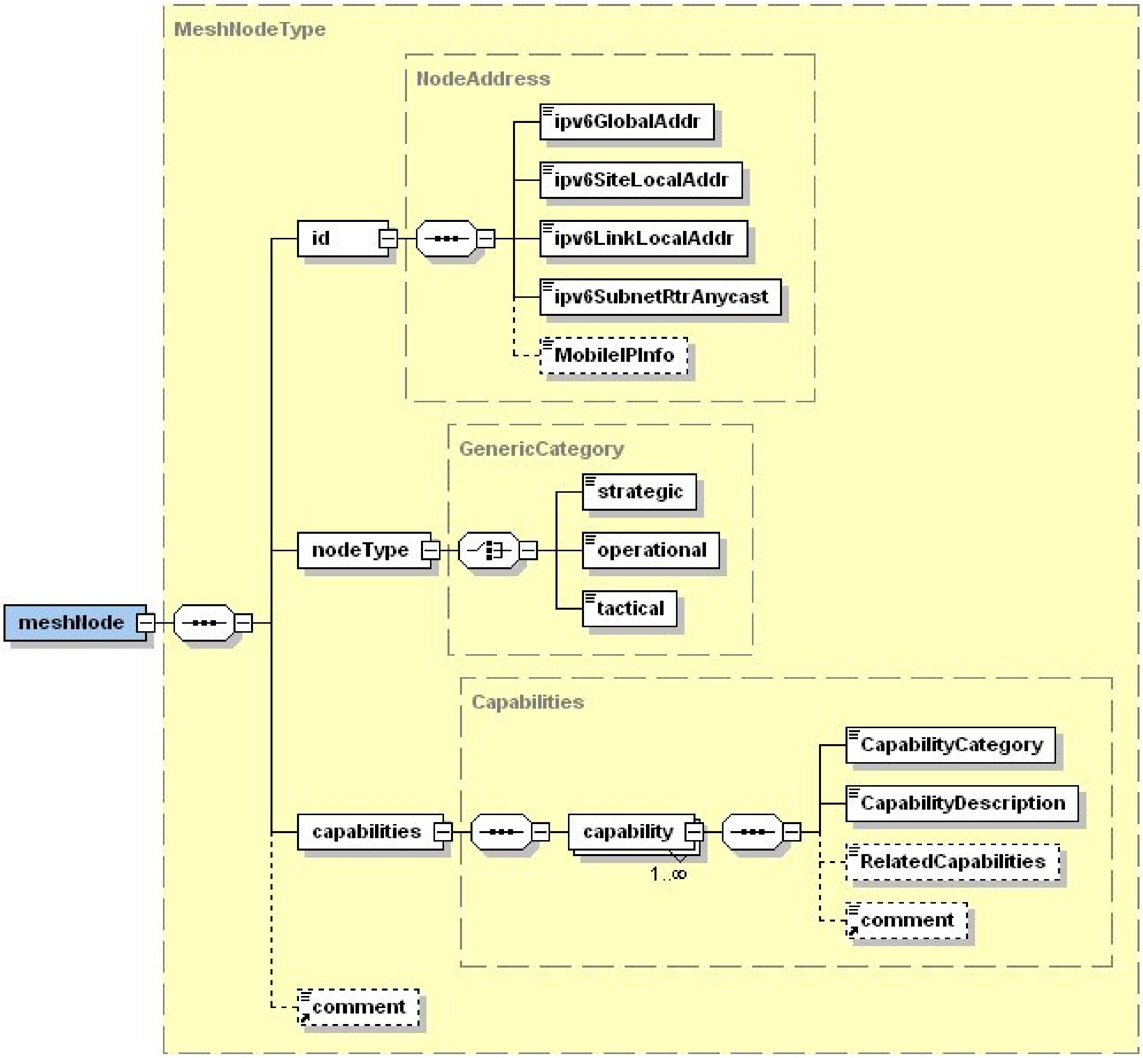


Figure 22. Sample MeshNetML Schema

theory. Many network-aware applications are already exchanging socket-layer deconfliction data, so an XML-derivative would add little in the way of overhead. Then, as the mechanism evolves and becomes validated as the glue for intra-GIG communications, required inclusion of the generic, product-line components into future large-scale applications should become the goal.

VI. FUTURE GIG MESH APPLICATIONS AND IMPLEMENTATION RECOMMENDATIONS

A. OVERVIEW AND RATIONALE

Based on nearly a year's worth of testing and experimentation data, we envision the GIG using wireless mesh networks in three distinct ways in the next five to ten years. First, we see a niche developing for base-level information technology data transfer mechanisms that would minimize the infrastructure investment involved with wireline networks. Second, we see infrastructure security applications as the first tier of a defense-in-depth strategy that could leverage several levels of wireless mesh. Finally, and most ambitiously, we foresee the emergence of workable agent-based and application layer management of the information within the mesh in order to radically transform the battlespace of the future.

B. BASE-LEVEL INFORMATION TECHNOLOGY SOLUTIONS

In a resource-constrained environment where every information technology purchase must be optimally procured for cost and benefit to the organization, fixed wireless mesh networking offers return on investment from the moment the first mesh access point is installed. By reducing the need for vulnerable cabling and other wiring closet hardware, a well-planned mesh solution could offer flexibility and cost-savings for any base-level information technology support directorate.

By moving the wired administrative networks towards a wireless mesh, military bases of the future would not only spend less capital, but could be rapidly reconfigured to accommodate workforce shifts or infrastructure expansion. A wireless mesh architecture could simplify the NOC management tasks, resulting in less personnel to administer and maintain the network. Additionally, visiting personnel could easily connect to the base network and the mesh solution could afford them mobile, seamless connectivity.

C. INFRASTRUCTURE PHYSICAL SECURITY

An ideal application environment for meshed sensors and geographically dispersed, higher-functioning "join points" is in the area of infrastructure physical security. Meshed perimeter security sensors could provide a virtual tripwire that could enhance a force protection posture almost immediately. Coupled with guard post or headquarters "join points" with identification and authentication tools, infrastructure security would undergo its first major advancement since the advent of security cameras.

The range of sensors that are emerging make this environment the most likely entry point for mesh within the GIG. Remotely-controlled visible and infrared cameras, seismic anomaly detectors, and audibly triggered devices are all categories of sensors that have achieved a level of maturity that is acceptable for immediate integration. The aggregation and translation mechanisms, mentioned earlier, are also becoming reality.

Figure 23 below illustrates the concept of using mesh to create a defense-in-depth, layered, physical security perimeter. The exterior, unattended ground sensors represent an alerting tripwire, and the next layer represents cameras and acoustic detectors. All the sensors have multiple-path reachback to the aggregating guard posts and the headquarters element. Because of the redundancy and robustness achieved through the use of a properly designed, securely implemented wireless mesh, security personnel are able to maintain a higher level of situational awareness and a better operational picture.

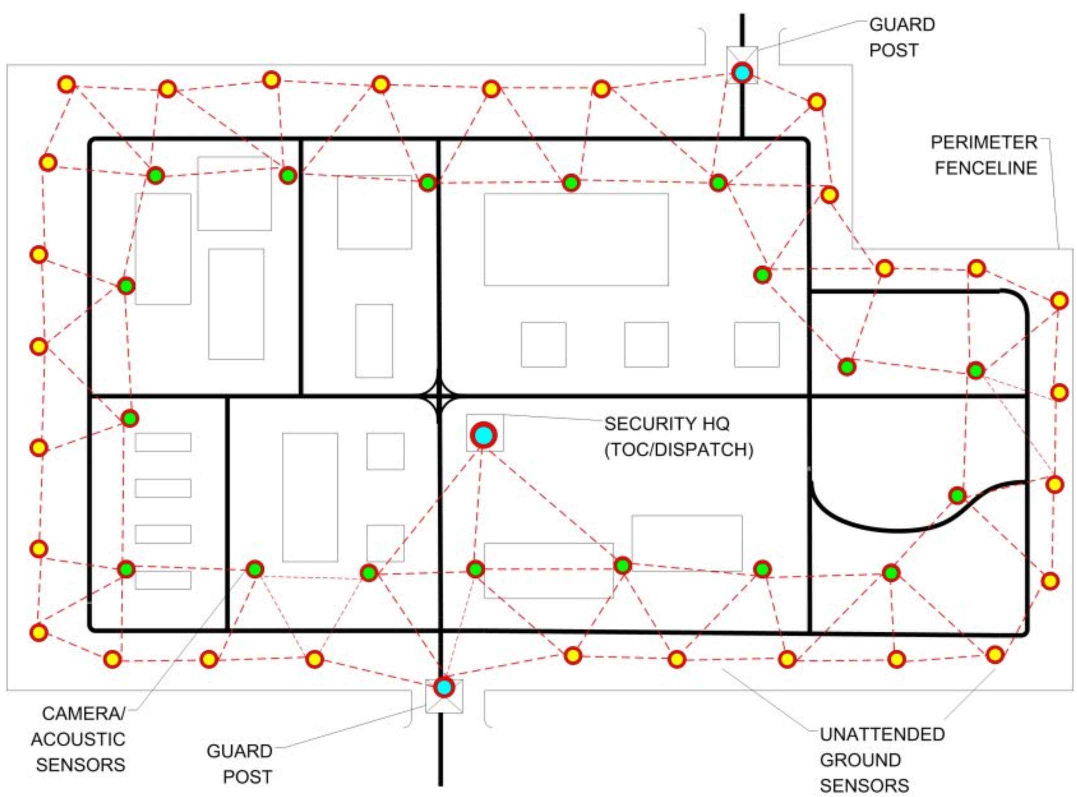


Figure 23. Notional Base Perimeter Security Mesh Network

D. BATTLESPACE OF THE FUTURE

The "true calling" of wireless mesh networking lies in its utility to radically transform the battlespace of the future and become an information superiority enabling technology within the GIG. The path toward this transformation will most likely leverage a services-derived architecture like MERCAT/MeshNetML in order to facilitate revolutionary new concepts like pervasive, device-aware networking and model-based communication networks for eventual end-to-end, near real-time situational awareness throughout the battlespace.

1. Device-Aware Networking (DAN)

The concept of Device-Aware Networking, "a network framework that supports device profile discovery and prevents unusable data from being delivered," is related to parts of the theory behind MERCAT, yet introduces the concept of "repurposing" to tailor content and data to the capabilities contained within the end nodes.[41]

Device-Aware Networks are intended to perform two major services. The first is sharing device capabilities on the network, and the second is a guarantee that data reaching another node will be usable by that node. This second element is the aforementioned repurposing task.

The capability discovery mechanism described by Singh, et al, is geared towards knowing the capability of an end node with respect to being able to handle some sort of incoming data. Once a node's capabilities are known, a method for patterning and processing the delivery of content to that node is invoked.[42] The services contained in the DAN framework, if architected correctly, may be viable, reusable components that could be leveraged for use in other frameworks that deal specifically with mesh networking.

2. Model-based Communication Networks (MCNs)

If mechanisms like MERCAT and DAN are even moderately successful in their implementation, the mesh networked battlespace of the future will be full of information.

[41] Su Wen and others, "Towards Device Aware Networks," in *Proceedings of the Twelfth International Conference on Telecommunications Systems*, July 2004, 321.

[42] Ibid, 325.

Indeed, there will be so much data passing across the network that information glut is likely to become the major stumbling block to effective communication between and amongst nodes. One proposed approach to handling the flood of bits and bytes is a "model-based communication network."[43]

The theory behind MCNs is that collaborating entities need a way to intelligently winnow the mass of incoming information and keep the most highly relevant and important elements. By using a filter-like, agent-based mechanism to analyze the data inputs, a service can be created that will deliver just the relevant, important information at the time it is needed. This concept is known as "valued information at the right time," or VIRT. One proposed architecture, outlined by Professor Rick Hayes-Roth of NPS, is composed of generic components that do plan monitoring and intelligent filtering based on defined parameters in a shared ontological framework. This is the essence of VIRT and the theory foundation behind MCNs.[44] Coupled with the always-on promise of mesh networks, the combination may be the symbiosis that truly leads to a revolution in military operations.

3. End-to-end Situational and Network Awareness

Lower-layer routing mechanisms, coupled with application layer, agent-based collaboration and communication services portend a level of situational awareness for the warrior of the future that eclipses what is possible, today. If intimately bound with the theory of properly focused information push and pull mechanisms, mesh networking becomes the instrument to enhance the warfighter's view of his world and far outpace an enemy's decision cycle.

Embedded network awareness will also be a force-multiplier as topologies rapidly change and self-configure. A "network awareness model" that includes agent-based, near real time network feedback would help increase the cognitive responsiveness of an active participant.[45] With knowledge of the surrounding capabilities of the fluid network, the

[43] Rick Hayes-Roth, "Model-based Communication Networks: Filtering Information by Value to Improve Collaborative Decision Making," Unpublished paper dated 09 July 2004, 1.

[44] Ibid, 9.

[45] A. Bordetsky, S. Hutchins, W. Kemple and E. Bourakov, "Network Aware Tactical Collaborative Environments," in *Proceedings of the Ninth International Command and Control Research and Technology Symposium*, 14 September 2003, 8.

mobile warrior of the future will be able to leverage the strengths and plan for the weaknesses within the fabric of the mesh. Initial implementations may involve network management tasks being pushed down to every node, but as application layer intelligence improves, the network awareness and management tasks will be handled by intelligent agents and services that create a seamless, always-on, optimized user experience that maximizes every single element and interface within the GIG.

E. ARCHITECTURE PLANNING RECOMMENDATIONS

Before attempting to implement a usable mesh networking framework within the GIG, a detailed, overarching architecture needs to be erected in order to address exactly how mesh concepts and technologies will be used and integrated across the spectrum of the GIG. A haphazard collection of meshed elements will result in nothing more usable, and perhaps something with less utility, than the infrastructure wireless efforts made to date. Both the Federal Enterprise Architecture Framework and the GIG Architecture provide a good starting point from which to develop a viable, executable sub-architecture that meets the needs of the warfighter of today and tomorrow.

We recommend development of an architecture built on specific use cases and scenarios that will be sufficiently forward-looking in order to build toward GIG goals as envisioned in the GIG Architecture, Version 2.0. The GIG Architecture Master Plan specifies that the GIG Architecture must, above all, "provide value to the warfighter."[46] Similarly, we believe the design and integration of wireless mesh components needs to be coordinated by a central activity, research lab, or a designated mesh networking center of excellence in order to maximize that value.

F. INVESTMENT RECOMMENDATION – A SPECIFIC BUSINESS CASE FOR MESH

In addition to the high-level architectural planning task for mesh across the GIG, we also recommend a rigorous business case be completed for each proposed implementation. While mesh may be the best fit for many future networking tasks, there are some situations that may be better served by the use of traditional wired or wireless networks. Infrastructures that depend on very high data throughput, absolute security

[46] Department of Defense, "Global Information Grid (GIG) Architecture Master Plan," 29 November 2002, 27.

from successful attacks, classified environments, and installations that have robust, modern wired backbones may not be viable candidates for a mesh replacement. Using the general case from Chapter III as an example, we completed a study of the wireless networking segment of NPS to determine if, indeed, a mesh solution would be advantageous.

NPS currently utilizes an extensive wired network with a recently-added wireless segment. The wireless segment is constantly expanding as more and more students and faculty desire wireless connectivity. The wireless network is currently composed of 70 traditional wireless access points (WAPs), creating multiple hotspots. These WAPs are connected to 35 high-speed Foundry switches through CAT5 Ethernet cable. These switches are then connected through CAT5 cable to 15 Foundry switches operating at the network "borders" (usually one or more per building), which consolidate all traffic. The border switches are then connected to the Network Operations Center through gigabit fiber optic cable and thence to the outside Internet. A rough cost breakdown is in Table 4 below:

First Year Startup Costs	Hotspots	Wireless Mesh Network
Equipment - Hotspots: 70 WAPs, 35 Foundry switches, 15 Foundry switches with Gigabit backhaul (borders) - Mesh: 70 WAPs, 15 aggregator WAPs Assumptions: - Cisco 1200 WAP family, $800 each, Foundry FastIron family, $2,000 each, Foundry ServerIron family, $6,000 each - Open architecture Mesh WAPs, $500 for outside aggregator WAPs, $470 for inside WAPs	**$216,000**	**$40,400**
Installation - 70 WAPs, 35 Foundry switches, 15 Foundry switches (borders), 70 Cat5e Ethernet runs from WAPs to switches, 35 Cat5e Ethernet runs from switches to border switches, 15 fiber optic cable runs from border switches to NOC - 70 Wireless Mesh APs, 15 aggregator Wireless Mesh APs for Wireless Mesh Network, Three Cat5e runs from three aggregator Mesh APs to NOC - Assumptions: 1 hour/Cat5e run, 12 hours/fiber run, 30 minutes/WAP, 30 minutes/switch, 1 hour/aggregator WAP, $50/hour	**$18,500**	**$2,275**
NOTE: All prices are estimates, and Internet connectivity costs are the same for the traditional and mesh and so were not included.		
Total first year expense – backhaul & installation	**$234,500**	**$42,675**

Table 4. NPS Business Case Summary Data

While we acknowledge that a fully engineered solution would consider other factors such as traffic and user population density, among others, our brief study indicated that an installation such as NPS could save $191,825 by implementing a wireless mesh networking solution over a more traditional wireless hotspot solution.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. CONCLUSION

A. CURRENT STATE OF TECHNOLOGY

Most current work and research in industry has been focused on the design and simulation of Layer 3 mesh protocols. Some effort has been made to leverage the application layer to anticipate and accommodate the unique nature of mesh networking, but much remains to be discovered. Fixed, community mesh initiatives are exploding as the technical challenges give way to economic and usability benefits. Emerging standards such as 802.11s and 802.16 (with mesh extensions) signal a maturity level that can and should be leveraged in the very near future. Mobile solutions are much less developed simply by virtue of the complexity of the problem space. In contrast, within the unattended sensor world, mesh is becoming a deployable reality, today.

B. CONCLUSIONS

It is undeniable that the issues of lower-layer mesh networking must be solved before real progress can be made in transforming application layer mesh into the enabling technology of the GIG. While research continues into the feasibility of wireless mesh networking at Layer 3, there is little work being done to erect an open architecture framework for information usability across the spectrum of users.

1. Feasibility of 802.x Mesh Products Within the GIG

From our research and observations, current 802.x wireless mesh offerings are still too immature with respect to security, stability, and reliability to be integrated into the GIG for the warfighter in the field. The level of robustness has not yet been achieved that would make us feel comfortable recommending sending troops into harm's way with industry standard meshed 802.11, 802.15.4, or 802.16 gear. For each and every experimental success we enjoyed, we encountered at least twice as many failures and challenges. While a cutting-edge solution may occasionally be appropriate to solve an urgent need, a more solidly engineered approach is necessary for field-grade, sustainable systems.

Emerging commercial product lines and standards, however, come much closer to meeting the robustness and security levels that need to be satisfied before mesh within the

GIG becomes a reality. Additionally, some lower data rate sensor meshes appear usable in their current form. However, further investigation in all major mesh categories is required before wider GIG employment is considered.

2. Applicability Generalizations

As we have previously outlined, the GIG could benefit from all three major divisions of 802.x wireless mesh networking technologies and the future fusion of diverse meshed communications paradigms. The opportunities for future mesh implementations are vast. The one true enabling technology to realizing the vision of the GIG, the end-to-end networked continuum, is wireless mesh networking.

Fixed wireless mesh networking systems offer rapidly deployable, readily reconfigurable, easily maintainable solutions to a constantly evolving and geographically shifting battleforce.

Mobile wireless mesh networking systems are the key to collaborative, augmented situational awareness through the promise of pervasive and ubiquitous computing connectivity.

Wireless sensor mesh systems offer the benefits of increased intelligence and early indications and warnings for targeting enemy assets as well as increasing the force protection posture of the battleforce.

All of the aforementioned approaches are applicable and highly relevant to the transformation towards network-centric warfare and the quest for information superiority.

C. RECOMMENDATIONS FOR FUTURE RESEARCH

Near-term future research should properly address four main areas. They include: (a) network layer protocol best-of-breed analysis for usability across the GIG environment; (b) investigation on the integration of robust security mechanisms; (c) further definition and refinement of MERCAT using MeshNetML as an enabling technology and XML vocabulary; and, (d) attempt to design and build the overarching architecture for integration into the multiple levels of the GIG.

Additionally, as the refinement and global adoption of wireless mesh networking continues, the potential for use by adversaries increases as well. Research on the possible exploitation of these networks should be undertaken to counter this future threat.

THIS PAGE INTENTIONALLY LEFT BLANK

SELECTED BIBLIOGRAPHY

"Cerritos Aims for Citywide Wi-Fi." *Federal Computer Week*. Available from http://www.fcw.com/geb/articles/2003/1208/web-cerritos-12-08-03.asp. Last Accessed 31 August 2004.

"Getting a Mesh Network to Work in the Real World Takes Some Work." *Techdirt* (August 29, 2003). Available from http://www.techdirt.com/articles/20030829/1359208.shtml. Last Accessed 13 September 2004.

"Mesh Networks Winning Converts." *Network World* (May 3, 2004). Available from http://www.nwfusion.com/news/2004/0503mesh.html. Last Accessed 13 September 2004.

"Sensor Model Language (SensorML)" (February 26, 2004). Available from http://vast.uah.edu/SensorML/. Last Accessed 13 August 2004.

"Wireless 'mesh' networks." *Surfability*. Available from http://www.surfability.com/ITC/mesh.php. Last Accessed 13 September 2004.

"Wireless Mesh Networks." *Sensors* (February 2003). Available from http://www.sensorsmag.com/articles/0203/38/main.shtml. Last Accessed 31 July 2004.

802.11b Mesh Access Point. Electronic document available from http://www.aerial-broadband.com/catalog/802_11b_mesh_access_point_1070929.htm. Last Accessed 13 September 2004.

Ad hoc On-Demand Distance Vector Routing. Electronic document available from http://moment.cs.ucsb.edu/AODV/aodv.html. Last Accessed 13 September 2004.

Basic Research Group. *Mobility Management for Heterogeneous Networks.* Available from http://cs.itd.nrl.navy.mil/5521/mmhn.html. Last Accessed 13 September 2004.

Beyer, Dave, Nico van Waes and Carl Eklund. *802.16 Mesh Extensions – Overview* (March 2002). Available from http://www.ieee802.org/16/tga/contrib/S80216a-02_30.pdf. Last Accessed 29 August 2004.

Blackshear Jr., Henry L. "Developing a Conceptual Unmanned Aerial Vehicle Communications Mobile Ad Hoc Network Simulation Model." Master's thesis, Naval Postgraduate School, June 2002.

Blackwell, Gerry. "Mesh Networks: Disruptive Technology?" *internetnews.com* (January 25, 2002). Available from http://www.wi-fiplanet.com/columns/article.php/961951. Last Accessed 13 September 2004.

Blazevich, Ryan J. "Wireless, Long Haul, Multi-Path Networking: Transforming Fleet Tactical Network Operations with Rapidly Deployable, Composable, Adaptive, Multi-Path Networking in Austere Environments." Master's thesis, Naval Postgraduate School, September 2004.

Bordetsky, A., S. Hutchins, W. Kemple and E. Bourakov. "Network Aware Tactical Collaborative Environments." In *Proceedings of the Ninth International Command and Control Research and Technology Symposium*, 14 September 2003.

Bosch, Jan. *Design and Use of Software Architectures.* London: Pearson Education, 2000.

Botts, Mike. *Overview of the SensorML UML Models.* Unpublished draft available from http://vast.nsstc.uah.edu/SensorML/SensorML_UML.doc. Last Accessed 5 September 2004.

Botts, Mike. *Sensor Model Language (SensorML) Version 0.6.* Electronic Presentation available from http://vast.nsstc.uah.edu/SensorML/SensorML.ppt. Last Accessed 4 September 2004.

Bowman, Cliff. "Wireless, Embedded Devices Find Common Ground in Mesh Network." *EE Times* (April 18, 2003). Available from http://www.eetimes.com/design_library/esd/cn/OEG20030418S0027. Last Accessed 13 September 2004.

Brenner, Pablo. "A Technical Tutorial on the IEEE 802.11 Protocol," BreezeCOM Whitepaper. BreezeCOM Wireless Communications, 1997.

Bulk, Frank. "Understanding Wireless Mesh Networks: Part 1." *Mobilepipeline.com* (June 09, 2004). Available from http://www.mobilepipeline.com/howto/21600011. Last Accessed 13 September 2004.

Carey, Patrick. *New Perspectives on XML-Comprehensive*. Boston: Course Technology, 2004.

Chandra, Ranveer, Christof Fetzer and Karin Hogstedt. "A Mesh-Based Robust Topology Discovery Algorithm for Hybrid Wireless Networks." In *Proceedings of Ad-Hoc Networks and Wireless (ADHOC-NOW 2002)*, September 2002.

Chee, Melissa. *The Business Case for Wireless Mesh Networks* (11 December 2003). Electronic presentation available from http://www.nortelnetworks.com/corporate/events/2003d/wmn_eseminar/. Last Accessed 5 September 2004.

Chen, Kam. "On the Road with the Mobile Mesh: Military Technology Could Help Alleviate Traffic Problems." *The Golden Gate [X]pressOnline* (October 22, 2003). Available from http://xpress.sfsu.edu/archives/tech/000236.html. Last Accessed 13 September 2004.

Cisco Systems. "Cisco 3200 Series Wireless and Mobile Routers." Electronic brochure available at http://www.cisco.com/en/US/products/hw/routers/ps272/prod_brochure_list.html, Last Accessed 6 September 2004.

Cisco Systems. *Cisco Networking Academy Program CCNA 1 and 2 Companion Guide.* Indianapolis: Cisco Press, 2003.

Comer, Douglas. *Computer Networks and Internets, with Internet Applications*. Upper Saddle River, NJ: Prentice Hall, 2001.

Corson, S. and J. Macker. "Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations." *Network Working Group* (January 1999). Request for Comments: 2501. Available from http://www.ietf.org/rfc/rfc2501.txt. Last Accessed 13 September 2004.

Cox, John. "Start-Up Joins WLAN Fray with Device." *Network World Fusion* (June 30, 2003). Available from http://www.nwfusion.com/news/2003/0630strix.html Last Accessed 14 September 2004.

Crossbow Technology. *Motes, SmartDust Sensors, Wireless Sensor Networks.* Available from http://www.xbow.com/Products/productsdetails.aspx?sid=3. Last Accessed 5 September 2004.

Das, Samir, Charles E. Perkins and Elizabeth M. Royer. "Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks." *INFOCOM 2000*, 2000.

Department of Defense Directive 8100.1. "Global Information Grid Overarching Policy." Dated 19 September 2002.

Department of Defense. "Global Information Grid (GIG) Architecture Master Plan." 29 November 2002.

Draves, Richard, Jitendra Padhye and Brian Zill. "Comparison of Routing Metrics for Static Multi-Hop Wireless Networks." *Microsoft Technical Report MSR-TR-2004-18.* Redmond, WA: Microsoft Corporation, 2004.

Ember Corporation. "Ember Product Family." Available from http://www.ember.com/products/family/index.html. Last Accessed 5 September 2004.

Exponent Corporation. "Land Warrior Program." Available from http://www.exponent.com/practices/techdev/landwarrior/index.html. Last Accessed 06 September 2004.

FastLine Mesh Networks home page. Available from http://www.fastlineinternet.com/. Last Accessed 13 September 2004.

Firetide: Wireless Instant Networks home page. Available from http://www.firetide.com/. Last Accessed 13 September 2004.

Geier, Jim. "Understanding Ad Hoc Mode" *Wi-Fi Planet* (August 23, 2002). Available from http://www.wi-fiplanet.com/tutorials/article.php/1451421. Last Accessed 13 September 2004.

Gerla, M., K. Xu and X. Hong. "Exploiting Mobility in Large Scale Ad Hoc Wireless Networks." *IEEE Computer Communication Workshop*, Dana Point, CA, 2003.

Gerla, Mario, Kaixin Xu, and Xiaoyan Hong. "Exploiting Mobility in Large Scale Ad Hoc Wireless Networks." *IEEE Computer Communication Workshop (CCW'03),* Dana Point, CA, October 2003.

Gerla, Mario, Xiaoyan Hong, and Guangyu Pei. "Landmark Routing for Large Ad Hoc Wireless Networks." *GLOBECOM 2000 - IEEE Global Telecommunications Conference, no. 1,* November 2000, 1702 – 1706.

Ghassemian, Mona, Phillipp Hofmann, Christian Prehofer, Vasilis Friderikos, and A. Hamid Aghvami. "Performance Analysis of Internet Gateway Discovery Protocols in Ad Hoc Networks." In *Proceedings of IEEE Wireless Communications and Networking Conference*, March 2004, 120-125.

Gohring, Nancy. "Motorola to Intro Wi-Fi/Cell Phone." *Wi-Fi Networking News* (27 July 2004). Available from http://wifinetnews.com/archives/004033.html. Last Accessed 13 September 2004.

Goodwins, Rupert. "Intel Makes a Mesh of Wireless Networks." *ZD Net* (February 21, 2003). Available from http://news.zdnet.com/2100-9584_22-985502.html. Last Accessed 13 September 2004.

Griffith, Eric. "FireTide Shows Off Mesh Router." *Wi-Fi Planet* (September 17, 2003). Available from http://www.wi-fiplanet.com/news/article.php/3078631. Last Accessed 13 September 2004.

Griffith, Eric. "Mesh Standard on the Starting Block." *DevX.com* (January 16, 2004). Available from http://www.devxnews.com/article.php/3300571. Last Accessed 13 September 2004.

Groove Virtual Office. Product Backgrounder, July 2004. Available from http://www.groove.net/pdf/backgrounder/GVO-backgrounder.pdf. Last Accessed 8 September 2004.

Halvardsson, Mattias and Patrik Lindberg. "Reliable Group Communication in a Military Mobile Ad hoc Network." Master's Thesis, Vaxjo University, February 2004.

Hauser, Jim, Dennis Baker and W. Steven Conner. "Draft PAR for IEEE 802.11 ESS Mesh" (14 November 2003).

Hayes-Roth, Rick. "Model-based Communication Networks: Filtering Information by Value to Improve Collaborative Decision Making." Unpublished paper dated 9 July 2004.

Hong, Xiaoyan, Mario Gerla, Guangyu Pei and Ching-Chuan Chiang, "A Group Mobility Model for Ad HocWireless Networks," *Proceedings of IEEE GLOBECOM 2000*, November 2000.

Howse, Martin. "Caught in the Mesh." *Linux User & Developer Magazine* 27 (March 2003).

Intel Corporation. "Deep Networking: Heterogeneous Sensor Networks." Available from http://www.intel.com/research/exploratory/heterogeneous.htm. Last Accessed 13 September 2004.

Intel Corporation. "Heterogeneous Sensor Networks." Available from http://www.intel.com/research/exploratory/heterogeneous.htm. Last Accessed 13 September 2004.

International Telecommunications Union. *Mesh Networks; ITU Strategy and Policy Unit Newslog*. http://www.itu.int/osg/spu/newslog/categories/meshNetworks/. Last Accessed 13 September 2004.

Ixia Corporation. "Qcheck – Network Performance Measurement." Available from http://www.ixiacom.com/products/performance_applications/pa_display.php?skey=pa_q_check. Last Accessed 29 August 2004.

Johnson, David B., David A. Maltz, Yih-Chun Hu. "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks." Internet-Draft Work in Progress, IETF MANET Working Group, 15 April 2003.

Kewney, Guy. "Features - Mesh Creator to be Overturned by the Big Guys?" *NewsWireless.net* (September 12, 2003). Available from http://www.newswireless.net/articles/031209-mesh.html. Last Accessed 13 September 2004.

Kewney, Guy. "Become a wireless ISP: for three hundred pounds." *NewsWireless.net* (January 20, 2003). Available from http://www.newswireless.net/articles/030120-locust.html. Last Accessed 13 September 2004.

Kinney, Patrick. "ZigBee Technology: Wireless Control that Simply Works." *Communications Design Conference*, October 2003. Available from http://www.zigbee.org/resources/documents/ZigBee_Technology_Sept2003.doc. Last Accessed 8 September 2004.

Klein-Berndt, Luke. "A Quick Guide to AODV Routing." Electronic publication available from http://w3.antd.nist.gov/wctg/aodv_kernel/aodv_guide.pdf. Last Accessed 13 September 2004.

Krag, Tomas and Sebastian Büettrich. "Wireless Mesh Networking." *O'Reilly Wireless Devcenter* (January 22, 2004). Available from http://www.oreillynet.com/pub/a/wireless/2004/01/22/wirelessmesh.html?page=last. Last Accessed 13 September 2004.

Larman, Craig. *Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and the Unified Process.* Upper Saddle River, NJ: Prentice Hall PTR, 2002.

Larsson, Tony and Nicklas Hedman. "Routing Protocols in Wireless Ad-Hoc Networks – A Simulation Study." Master's thesis, Lulea University of Technology, 1998.

Lee, Sung-Ju, J. Hsu, R. Hayashida, M. Gerla, and R. Bagrodia. "Selecting a Routing Strategy for your Ad Hoc Network." *Computer Communications* 26, no. 7 (May 2003).

List, William and Nitin Vaidya. "A Routing Protocol for k-hop Networks." In *Proceedings of IEEE Wireless Communications and Networking Conference*, March 2004, 2545-2550.

Liu, Yu and Jack Lau. "A Novel Link State Routing Protocol and TCP Performance Investigation in Ad Hoc Networks." In *Proceedings of IEEE International Conference on Networks*, Singapore, August 2002.

LocustWorld home page. Available from http://www.locustworld.com. Last Accessed 13 September 2004.

LocustWorld. "Mesh in Columbia Gorge – Washington State, USA." Available from http://locustworld.com/modules.php?op=modload&name=News&file=article&sid=35. Last Accessed 31 August 2004.

LocustWorld. "The Information Revolution – Mesh Networking Hardware and Software." Available from http://locustworld.com/index.php. Last Accessed 3 September 2004.

Lofgren, Thomas. "Evaluation of the CEDAR Routing Algorithm in MANET Scenarios." Master's thesis, Uppsala University, 4 June 1999.

Mannion, Patrick. “Wireless Mesh Networking Gathers Momentum.” *EE Times* (November 10, 2003). Available from http://www.commsdesign.com/story/OEG20031110S0077. Last Accessed 13 September 2004.

Mannion, Patrick. “Wireless Mesh Networks Gain Traction.” *EE Times* (November 17, 2003). Available from http://www.commsdesign.com/news/tech_beat/OEG20031117S0037. Last Accessed 13 September 2004.

McGrath, Sean. “The Wireless Mesh-Men Cometh.” *IT World*, Ebusiness in the Enterprise issue (April 1, 2003). Available from http://www.propylon.com/news/ctoarticles/wireless_mesh_030408.html. Last Accessed 13 September 2004.

Merritt, Rick. “Cisco, Intel to Push Wireless Mesh Standard.” *EE Times (*December 5, 2003). Available from http://www.cmpnetasia.com/ViewArt.cfm?Artid=22365&Catid=5&subcat=60. Last Accessed 13 September 2004.

MeshDynamics home page. Available from http://www.meshdynamics.com/index.html. Last Accessed 13 September 2004.

MeshDynamics, “Why Structured Mesh is Different.” Available from http://www.meshdynamics.com/WhyStructuredMesh.html. Last Accessed 14 September 2004.

MeshDynamics. *OEM Ready Mesh Neworking Software.* Available from http://www.meshdynamics.com/wPresentations.html. Last Accessed 13 September 2004.

MeshNetworks home page. Available from http://www.meshnetworks.com/index.htm. Last Accessed 13 September 2004.

MITRE Corporation. *Our Work – Technology Tranfer – Mobile Mesh*. Last Updated 08 October 2003. Available from http://www.mitre.org/work/tech_transfer/mobilemesh/. Last Accessed 13 September 2004.

Morrissey, Brian. “The Next 802.11 Revolution?” *internetnews.com*. Available from http://www.internetnews.com/wireless/article.php/1365611. Last Accessed 13 June 2002.

Moskaluk, Inc. home page. Available from http://www.moskaluk.com/. Last Accessed 13 September 2004.

Motorola, Inc. “Motorola Turns Enterprise Business Communications Inside Out.” Motorola Press Release (27 July 2004). Available from http://www.motorola.com/mediacenter/news/detail/0,,4493_3826_23,00.html. Last Accessed 15 August 2004.

National Institute of Standards and Technology. *Wireless Ad Hoc Networks.* Available from http://www.itu.int/osg/spu/newslog/categories/meshNetworks/. Last Accessed 13 September 2004.

Nova Engineering, Inc. home page. Available from http://www.novaroam.com/inside.asp. Last Accessed 13 September 2004.

NOW Wireless Mesh Network: High Speed Internet Connection on the Move. Electronic document available from http://www.nowwireless.co.uk/NOW_Wireless_mesh.html. Last Accessed 13 September 2004.

Ogier, R., F. Templin, and M. Lewis. *Topology Dissemination Based on Reverse-Path Forwarding (TBRPF).* RFC 3684, Internet Engineering Task Force (IETF), February 2004.

PacketHop home page. Available from http://www.packethop.com/home.html. Last Accessed 13 September 2004.

Pei, G., M. Gerla, and X. Hong. "LANMAR: Landmark Routing for Large Scale Wireless Ad Hoc Networks with Group Mobility." In *Proceedings of IEEE/ACM MobiHOC 2000*, Boston, MA, August 2000.

Perkins, C., E. Belding-Royer, and S. Das. *Ad Hoc On-Demand Distance Vector (AODV) Routing.* RFC 3561, Internet Engineering Task Force (IETF), July 2003.

Perkins, Charles E. "Tutorial: MobileIP" (1997). Available from http://www.computer.org/internet/v2n1/perkins.htm. Last Accessed 6 September 2004.

Perkins, Charles, ed. *Ad Hoc Networking*. Boston: Addison-Wesley, 2001.

Pescovitz. David. "Sensing Nature's Ways: Tiny Sensors Keep a Watchful Eye on Remote Habitats." *Berkeley Engineering* (Fall 2003).

Poor. Robert. "Wireless Mesh Networks." *Sensors Online* (February 2003). Available from http://radio.weblogs.com/0105910/2003/03/01.html. Last Accessed 13 September 2004.

Proxicast Wireless Internet Service Provider (WISP) home page. Available from http://www.proxicast.com/WISP/. Last Accessed 13 September 2004.

Rotondo, Rick. "An Introduction to Mesh Networking." *Broadband Wirless Exchange Magazine.* Available from http://www.bbwexchange.com/news/2003/may/meshnetworks051903.asp. Last Accessed 13 September 2004.

Royer, E. M. and C-K Toh. "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks." *IEEE Personal Communications* (April 1999).

Rupley, Sebastian. "Wireless: Mesh Networks." *PC Magazine* (July 1, 2003). Available from http://www.pcmag.com/article2/0,4149,1130864,00.asp. Last Accessed 13 September 2004.

Rupley, Sebastian. "Wireless: Mesh Networks." *PC Magazine* (July 1, 2003). Available from http://www.pcmag.com/article2/0,4149,1130864,00.asp. Last Accessed 31 July 2004.

Schaumann, Jan, *Analysis of the Zone Routing Protocol* (8 December 2002). Electronic resource available from http://www.netmeister.org/misc/zrp/zrp.pdf. Last Accessed 9 September 2004.

Shea, Kevin M. "Simulation and Performance Analysis of the Zone Routing Protocol for Tactical Mobile Ad Hoc Networks." Master's thesis, Naval Postgraduate School, September 2000.

Sholander, Peter, Andreas Yankopolus, Paul Coccoli, and Siamak Tabrizi. "Experimental Comparison of Hybrid and Proactive MANET Routing Protocols." *IEEE Military Communications Conferences (MILCOM 2002)*, Anaheim, CA, October 2002.

Sholander, Peter, Paul Coccoli, Tracey Oakes and Sean Swank. "A Portable Software Implementation of a Hybrid MANET Routing Protocol." *Scientific Research Corporation Whitepaper*. Atlanta, GA: Scientific Research Corporation, 2002.

Sinclair, Matthew. "Wireless Mesh Networking; An Investigation into AODV Routing." Fourth-Year Computer Systems Engineering Project, Massey University, 2003.

Singer, Michael. "Wireless Mesh Standard Coming." *Wi-Fi Planet* (December 5, 2003). Available from http://www.wi-fiplanet.com/news/article.php/3285981. Last Accessed 13 September 2004.

Smith, Brad. "Mesh: It Works, But Will Anyone Use It?" *Wireless Week* (December 2, 2002). Available from http://www.wirelessweek.com/index.asp?layout=article&articleid=CA262324. Last Accessed 13 September 2004.

Stone, Adam. "Wireless Mesh Networks Making Gains." *IEEE Distributed Systems Online*. Available from http://dsonline.computer.org/0312/f/oz004a.htm. Last Accessed 13 September 2004.

Strix Systems home page. Available from http://www.strixsystems.com/. Last Accessed 13 September 2004.

Strix Systems. "Products." Available from http://www.strixsystems.com/products/products_main.asp. Last Accessed 3 September 2004.

Strix Systems. "Access/One Network Product Description." Available from http://www.strixsystems.com/downloads/product_description/Strix_prodescription_web.pdf. Last Accessed 2 September 2004.

Thomson, S., Bellcore and T. Narten. *IPv6 Stateless Address Autoconfiguration.* RFC 1971, Internet Engineering Task Force (IETF), August 1996.

Toh, C.-K. *Ad Hoc Mobile Wireless Networks: Protocols and Systems*. Upper Saddle River, NJ: Prentice Hall PTR, 2002.

Tonnesen, Andreas. "Implementing and Extending the Optimized Link State Routing Protocol." UniK University Graduate Center, University of Oslo, 1 August 2004.

Tropos Networks home page. Available from http://www.troposnetworks.com/technology/index.shtml. Last Accessed 13 September 2004.

Griffith, Eric. "Tropos: Supplier of Metro Wi-Fi." *Wi-Fi Planet* (May 21, 2003). Available from http://www.wi-fiplanet.com/news/article.php/2210711. Last Accessed 13 September 2004.

UltrameshWireless Networking home page. Available from http://www.ultramesh.com/. Last Accessed 13 September 2004.

Walker, P.E. Jonathan. "Wi-Fi Mesh Networks, the Path to Mobile Ad Hoc." *The Wi-Fi Technology Forum*, 2004.

Wang, Maoning. "MANET Global Connectivity and Mobility Management Using HMIPv6 and OLSR." Master's thesis, Carleton University, 23 August 2003.

Wen, Su, Gurminder Singh, John Gibson, and Arijit Das. "Towards Device Aware Networks." In *Proceedings of the Twelfth International Conference on Telecommunications Systems*, July 2004.

WiFi Hermosa Beach, "WiFi Hermosa Beach," Available from http://www.wifihermosabeach.com/. Last Accessed 31 August 2004.

WisperNet: Wireless Multi-Hop Mesh Network Platform. Electronic document available from http://www.ece.cmu.edu/wispernet/. Last Accessed 13 September 2004.

Xu, K., X. Hong, M. Gerla, H. Ly and D. Gu. "Landmark Routing in Large Wireless Battlefield Networks Using UAVs." In *Proceedings of IEEE MILCOM 2001*, 2001.

Xu, K., X. Hong, M. Gerla, H. Ly and D. Gu. “Landmark Routing in Ad Hoc Networks with Mobile Backbones.” *Journal of Parallel and Distributed Computing* 63, Issue 2 (February 2003): 15.

Xu, Kaixin and Mario Gerla. “A Heterogeneous Routing Protocol Based on a New Stable Clustering Scheme.” *IEEE Military Communications Conferences (MILCOM 2002),* Anaheim, CA, October 2002.

Xu, Kaixin, Ken Tang, Rajive Bagrodia, Mario Gerla, and Michael Bereschinsky. “Adaptive Bandwidth Management and QoS Provisioning in Large Scale Ad Hoc Networks.” *IEEE Military Communications Conferences (MILCOM)*, 2003.

Xu, Kaixin, Xiaoyan Hong, and Mario Gerla. “An Ad Hoc Network with Mobile Backbones.” I*EEE International Conference on Communications (ICC'02),* New York, NY, April 2002.

Xu, Kaixin, Xiaoyan Hong, Mario Gerla, Henry Ly, and Daniel Gu. “Landmark Routing in Large Wireless Battlefield Networks Using UAVs.” *IEEE Military Communications Conferences (MILCOM'01)*, Vienna, VA, October 2001.

Yi, Yunjung, Joon-Sang Park, Sungwook Lee, Yeng-Zhong Lee, and Mario Gerla. “Implementation and Validation of Multicast-Enabled Landmark Ad-hoc Routing (M-LANMAR) Protocol.” *IEEE Military Communications Conferences (MILCOM)*, 2003.

Yi, Yunjung, Xiaoyan Hong, and Mario Gerla. “Scalable Team Multicast in Wireless Ad Hoc Networks Exploiting Coordinated Motion.” *NGC*, 2002.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Alexander Bordetsky
   Naval Postgraduate School
   Monterey, California

4. Brian Steckler
   Naval Postgraduate School
   Monterey, California

5. Dan Boger
   Naval Postgraduate School
   Monterey, California

6. Eric Bach
   Naval Postgraduate School
   Monterey, California

7. Mark Fickel
   Naval Postgraduate School
   Monterey, California